NM Health Care Authority (HCA)
Artificial Intelligence (AI) Policy

Revision History

Revision Number	Revision Date	Summary of changes	By
Version 1	March 11, 2025	Initial version	Paula Morgan

I. Purpose

The purpose of this policy is to guide the responsible, ethical, and secure usage of ***Artificial Intelligence (AI)*** technologies within the New Mexico Health Care Authority (HCA). This policy, in conjunction with the application of organizational, state, and federal laws, regulations, and policies aims to establish an operational framework for protecting the assets, workforce, and users from potential risks (e.g., Cybersecurity Risks or ***AI Risks*****).**

II. Definition

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. (Source National Artificial Intelligence Act of 2020)

III. Scope

This policy applies to HCA *personnel*, *data*, systems, network(s), and applications seeking to integrate with or leverage AI technologies. The policy covers all divisions and offices within HCA and extends to third parties (e.g., vendors, contractors, etc.) providing services on behalf of HCA.

IV. Policy

The use of AI can bring significant business value to HCA. Following a responsible planning, implementation, solution monitoring, and reporting process will allow HCA to effectively manage technology and further align with organizational needs.

A. AI Solution Development

As part of AI Solution Development HCA shall follow the iterative activities outlined below:

Planning and Implementation

Planning and implementation practices shall be implemented to ensure the proper use and deployment of AI tools and resources. Planning and implementation practices shall include:

1. Defining a formal process for identifying, documenting, reviewing, and approving *AI use cases ('use cases')*.
2. HCA use cases and solutions shall be inventoried or reported annually and shall align with the NIST AI Risk Management Framework.
3. Submission of HCA approved use cases to the ITD Change Control Board (CCB) as appropriate.
4. Designing an approved use case pilot prior to full production implementation.
5. Providing comprehensive documentation on how data will be sourced, processed, managed, and stored.
6. Conducting any necessary data quality testing for pilot and full production of AI deployments, including:
   a) Reviewing and evaluating any AI-generated output for proper functionality and security.
   b) Evaluating the data sets for AI Models to determine the degree of operational compliance, and errors related to bias and variance.
   c) Testing activities shall be properly documented.
7. Defining the hand-off criteria to determine when judgment and decisions from an AI solution are transitioned to a human.
8. Charging human operators with reviewing AI outputs for accuracy, appropriateness, privacy, and security before being acted upon or disseminated. AI outputs shall not be assumed to be truthful, credible, or accurate.

AI Solution Monitoring and Use Case Reporting

1. Ongoing monitoring of AI generated output to validate that errors or data biases are not introduced as the model evolves.
2. The HCA Chief Information Security Officer will be required, as applicable, to identify which use cases are safety-impacting and rights-impacting AI and report additional detail on the risks—including risks of inequitable outcomes—that such uses pose and how they are managing those risks.
3. AI use cases must be individually inventoried at least annually, the inventory will be submitted to the ITD CCB.

B. Data Governance

Data Governance practices shall be implemented to ensure the proper handling (processing, managing, and/or storing), quality control, security, and privacy of data that is intended for AI solution development. Data Governance practices shall adhere to the following standards:

1. The HCA Data Governance Committee must approve the use of Personally Identifiable Information (PII), Protected Health Information (PHI), and controlled or sensitive organizational data prior to introducing it to any AI system(s).

2. Define guidelines for data collection, storage, and usage to ensure compliance with privacy regulations, data protection, and data quality standards.
3. AI models shall not be trained with data that is biased, inaccurate, incomplete, or misleading.
4. AI systems shall only have access to the data sources they need for the specific context.
5. Data shall be regulated through established data sharing agreements that identify the applicable federal and state laws and policies for the AI solution use case. The agreements shall outline the acceptable terms for data use, storage, and transmission.
6. Data sources used with AI shall be properly parsed into multiple, randomized data sets consisting of training, cross-validation, and test data.
7. Data validation procedures shall be in place to select, analyze, clean, and certify the integrity of the data sources that will be used for AI automation solutions.
8. Designated roles shall be responsible for maintaining the quality and integrity of AI models developed by or on behalf of HCA.

C. Acceptable Use

Acceptable use guidelines are established to ensure the lawful, ethical, and responsible use and development of AI technologies to safeguard HCA's professional reputation, brand, and compliance with regulations. Each personnel must adhere to the following principles when using or developing AI technology:

1. Use of AI technology for work purposes must be approved by HCA Strategy Team and must be in alignment with the requirements defined by the Data Governance Committee and ITD CCB.
2. Use of AI technology must be lawful and not jeopardize the department's professional reputation or brand.
3. Personnel are responsible for issues arising from their elective use of AI as part of business processes.
4. Privacy or data protection regulations must be respected and complied with when using AI systems.
5. AI outputs must not be manipulated or used to impersonate individuals or organizations without their written permission.
6. AI technology must not be used in lieu of special purpose business applications, to answer questions which require consultation with HCA leadership or subject matter advisors, or as the sole resource for questions.
7. Use of AI technology must be disclosed to HCA whenever being used to create deliverables.
8. Only approved data can be entered into AI technologies, and personnel must get approval to enter any Personal Health Information (PHI), Personal Information (PI), Personally Identifiable Information (PII), Personally Identifiable Information – Adoption Care Health Information (HI), Restricted (R), or sensitive organizational data.
9. Output provided by AI technologies must be verified by personnel for accuracy, completeness, and relevance. Any necessary edits must be made before sharing the output for any purpose.

D. Exceptions

Exceptions from certain policy provisions may be sought following the HCA exception process.

E. Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.