2024

Artificial Intelligence Regulatory Resource Guide

2024 Artificial Intelligence Regulatory Resource Guide

July 2024

Artificial Intelligence (AI) and its widespread applicability in healthcare became the center of health technology discussion in 2023. While used in various areas of healthcare for the better part of a decade, the release of easy to use, open-source machine learning and generative AI created an environment for rapid deployment of new technology. The US healthcare technology regulatory framework aims to provide limited guardrails for the use of AI in healthcare, however, gaps remain.

The Biden-Harris Administration has taken several steps to establish guardrails around the use of AI. That said, federal agencies have limited authority to regulate AI tools. As a result, agencies have attempted to provide guidance to the healthcare continuum despite limited statutory authority.

This toolkit provides an overview of the AI regulations related to healthcare that are in place, or proposed. This includes the Executive Order on AI released by the Biden-Harris Administration and the Office of Management and Budget (OMB) guidance for federal departments and agencies themselves, as well as agency regulation and guidance.

The AHIMA Policy & Government Affairs team continues to monitor the federal regulatory environment for developments and changes to the current government compliance framework. If you have questions or would like to discuss your experiences with AI and the regulatory implications, please contact us at advocacy@ahima.org.

This document will be updated as needed to reflect the AI regulatory landscape in Washington, DC.

Regulatory Agencies Included in Toolkit

Cybersecurity and Infrastructure Security Administration (CISA): CISA is the operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience.

Centers for Medicare & Medicaid Services (CMS): CMS is the federal agency that provides health coverage to more than 160 million beneficiaries through Medicare, Medicaid, the Children's Health Insurance Program, and the Health Insurance Marketplace. CMS works in partnership with the entire healthcare community to improve quality, equity, and outcomes in the healthcare system.

Food and Drug Administration (FDA): The FDA is responsible for protecting the public health by ensuring the safety, efficacy, and security of human and veterinary drugs, biological products, and medical devices; and by ensuring the safety of the nation's food supply, cosmetics, and products that emit radiation.

National Institute for Standards and Technology (NIST): The National Institute of Standards and Technology (NIST) is the nation's preeminent agency related to regulating new and innovative technologies. Under the US Department of Commerce, NIST's focus extends beyond the reaches of healthcare and is focused on all technology created and/or deployed within the US. NIST has an acute interest in AI, but does not have the regulatory authority to regulate AI tools. In the absence of such authority, NIST often releases frameworks that include recommendations on how best to develop such tools and products.

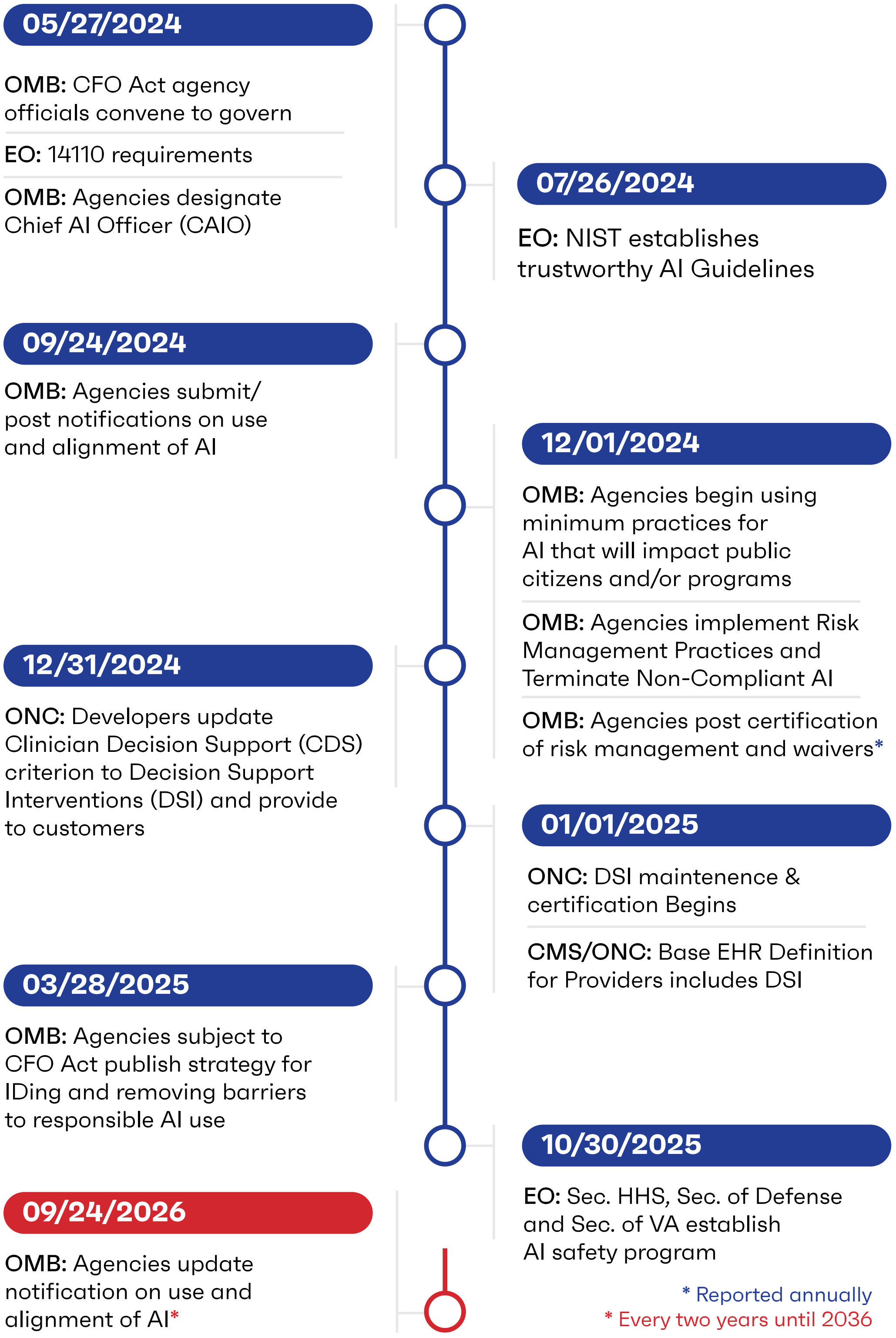
Office of Management and Budget (OMB): The OMB oversees the implementation of the President's vision across the Executive Branch. OMB carries out its mission through five main functions across executive departments and agencies: budget development and execution; management, including oversight of agency performance, procurement, financial management, and information technology; coordination and review of all significant federal regulations from executive agencies, privacy policy, information policy, and review and assessment of information collection requests; clearance and coordination of legislative and other materials, including agency testimony, legislative proposals, and other communications with Congress, and coordination of other Presidential actions; clearance of Presidential Executive Orders and memoranda to agency heads prior to their issuance.

Office of the National Coordinator for Health Information Technology (ONC): The ONC is at the forefront of the administration's health IT efforts and is a resource to the entire health system to support the adoption of health information technology and the promotion of nationwide, standards-based health information exchange to improve healthcare.

Artificial Intelligence Regulatory Enforcment Timeline

2024-2026

The below regulatory timeline includes a summary of relevant AI deadlines that may impact healthcare or healthcare related agencies contained in the referenced documents. This timeline does not include all deadlines in the referenced documents.



05/27/2024

OMB: CFO Act agency officials convene to govern

EO: 14110 requirements

OMB: Agencies designate Chief AI Officer (CAIO)

07/26/2024

EO: NIST establishes trustworthy AI Guidelines

09/24/2024

OMB: Agencies submit/ post notifications on use and alignment of AI

12/01/2024

OMB: Agencies begin using minimum practices for AI that will impact public citizens and/or programs

OMB: Agencies implement Risk Management Practices and Terminate Non-Compliant AI

OMB: Agencies post certification of risk management and waivers*

12/31/2024

ONC: Developers update Clinician Decision Support (CDS) criterion to Decision Support Interventions (DSI) and provide to customers

01/01/2025

ONC: DSI maintenence & certification Begins

CMS/ONC: Base EHR Definition for Providers includes DSI

03/28/2025

OMB: Agencies subject to CFO Act publish strategy for IDing and removing barriers to responsible AI use

10/30/2025

EO: Sec. HHS, Sec. of Defense and Sec. of VA establish AI safety program

09/24/2026

OMB: Agencies update notification on use and alignment of AI*

* Reported annually

* Every two years until 2036

FDA Role in AI Regulatory Oversight:

The FDA reviews medical devices through an appropriate premarket pathway, such as premarket clearance (510(k)), De Novo classification, or premarket approval. The FDA may also review and clear modifications to medical devices, including software as a medical device, depending on the significance or risk posed to patients of that modification.

Annual Agency Requirements:

- Inventory AI use cases
- Submit report on use cases to OMB and post publicly
- Report and release metrics about use cases

Referenced Regulatory Texts:

- Executive Order (EO) on the Safe, Secure, and Trustworthy Development and Use of AI
- OMB Memo Advancing Governance, Innovation, and Risk Management for Agency Use of AI
- ONC HTI-1

Executive Order on Safe, Secure, and Trustworthy AI

Released: October 30, 2023

Background

The Biden-Harris Administration released the Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence[1] on October 30, 2023. The Executive Order sought to use the Executive Branch's existing statutory authorities to regulate the use of AI both within and outside of the US Federal Government. A fact sheet[2] was released by the White House indicating the Executive Order sought to establish new standards for AI safety and security, protect Americans' privacy, advance equity and civil rights, stand up for consumers and workers, promote innovation and competition, advance American leadership, and address other key areas of focus.

While the Executive Order is the most aggressive piece of AI policymaking yet, it is noted that direction given to the agencies named within the Executive Order is subject to the availability of appropriations. Areas that need additional authorizations or appropriations to enact the directions contained within the Executive Order will require congressional approval. Nearly every Executive Branch Agency is named in the Executive Order, even though not named explicitly. For instance, several provisions allude to work the Office of the National Coordinator for Health Information Technology (ONC) has already undertaken.

Key Provisions within the Executive Order

- Identifies and defines key terms related to AI to provide harmony across the agencies;
- Requirements related to ensuring AI tools deployed and utilized are safe and reliable;
- Details updates and the development of best practices related to the cybersecurity of AI;
- Promotes innovation and competition in the development of healthcare AI;
- Includes plans related to protecting workers such as:
  - Identifying the impact of AI on the US workforce;
  - Protecting workers as AI is deployed and utilized;
  - Ensuring employee well-being is protected; and
  - Ensuring employee upskilling education is available.
- Details healthcare-specific AI activities within the US Department of Health and Human Services (HHS) including:
  - Creating an AI taskforce within HHS;
  - Determining if HHS sub-agencies are able to determine whether AI is reliable and safe and creating a plan to address identified issues; and
  - Creating an action plan to ensure AI is deployed and used in an equitable manner.

[1] Available at: https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/.
[2] Available at: https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/.

Key Definitions within the Executive Order

- **Artificial Intelligence (AI):** Defines AI[3] as 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.
- **AI Model:** A component of an information system that implements AI technology and uses computational, statistical, or machine-learning techniques to produce outputs from a given set of inputs.
- **Dual-use Foundation Model:** An AI model that is trained on broad data; generally uses self-supervision; contains at least tens of billions of parameters; is applicable across a wide range of contexts; and that exhibits, or could be easily modified to exhibit, high levels of performance at tasks that pose a serious risk to security, national economic security, national public health or safety, or any combination of those matters.
- **Generative AI:** The class of AI models that emulate the structure and characteristics of input data to generate derived synthetic content. This can include images, videos, audio, text, and other digital content.
- **Machine Learning:** A set of techniques that can be used to train AI algorithms to improve performance at a task based on data.
- **AI Red-Teaming:** A structured testing effort to find flaws and vulnerabilities in an AI system, often in a controlled environment and in collaboration with developers of AI, most often performed by dedicated “red teams” that adopt adversarial methods to identify flaws and vulnerabilities, such as harmful or discriminatory outputs from an AI system, unforeseen or undesirable system behaviors, limitations, or potential risks associated with the misuse of the system.

[3] Set forth in 15 U.S.C. 9401(3).

Office of Management and Budget Memorandum – Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence

Released: March 28, 2024

Background

On March 28, 2024, the US Office of Management and Budget (OMB) released a memorandum[4] for the heads of executive departments and agencies on Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence.

This memorandum establishes new agency requirements and guidance for AI governance, innovation, and risk management, including specific minimum risk management practices for uses of AI that impact the rights and safety of the public. Except as specifically noted, the memorandum applies to all executive branch agencies, but some requirements apply only to agencies identified in the Chief Financial Officers Act (CFO Act)[5].

Strengthening AI Governance: Each agency must designate a Chief AI Officer (CAIO) within 60 days of publication of the memorandum. The memorandum describes the roles, responsibilities, seniority, position, and reporting structures for agency CAIOs, and CAIOs must work in close coordination with existing responsible officials and organizations within their agencies.

- The CAIO will coordinate agency use of AI, promote AI innovation, and manage risks for their agency's use of AI specifically, as opposed to data or IT issues in general. The CAIO will convene relevant senior officials to coordinate and govern issues tied to the use of AI within the federal government.
- Within 180 days of this memorandum and every two years after, each agency must submit to OMB and post publicly on the agency's website either a plan to achieve consistency with this memorandum or a written determination that the agency doesn't use AI.
- The agency must inventory each of its AI use cases at least annually, submit inventory to OMB, post a public version on the agency's website, and annually report and release aggregate metrics about these use cases.
- Agencies' AI coordination mechanisms should be aligned to the needs of the agency based on, for example, the degree to which the agency currently uses AI, the degree to which AI could improve the agency's mission, and the risks posed by the agency's current and potential uses of AI.

[4] Available at: https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf.
[5] Available at: https://www.cio.gov/handbook/it-laws/cfo-act/.

- Each CFO Act agency is required to establish an AI governance board to convene relevant senior officials to govern the agency's use of AI, including to remove barriers to the use of AI and manage its associated risks.

Advancing Responsible AI Innovation: Agencies are encouraged to prioritize AI development and adoption for the public good and where the technology can be helpful in understanding and tackling large societal challenges, such as using AI to improve the accessibility of government services or improve public health.

- Each agency is required to develop and publicly post on the agency website an enterprise strategy for how they will advance the responsible use of AI, with recommendations for how agencies should reduce barriers to the responsible use of AI (e.g., barriers related to IT infrastructure, data, cybersecurity, workforce, generative AI).
- Agencies should create internal environments where those developing and deploying AI have sufficient flexibility and where limited AI resources and expertise are not diverted away from AI innovation and risk management.
- Agencies are strongly encouraged to prioritize recruiting, hiring, developing, and retaining talent in AI and AI-enabling roles to increase enterprise capacity for responsible AI innovation.
- Agencies must share their AI code, models, and data, and do so in a manner that facilitates re-use and collaboration government-wide and with the public.
- OMB and OSTP will coordinate the development and use of AI in agencies' programs and operations across federal agencies through an interagency council that will include promoting shared templates and formats, sharing best practices and lessons learned, sharing technical resources for implementation, and highlighting exemplary uses of AI for agency adoption.

Managing Risks from the Use of AI: This memorandum establishes new requirements and recommendations that address the specific risks from relying on AI to inform or carry out agency decisions. Agencies are required to follow minimum practices when using safety-impacting AI and rights-impacting AI, and enumerate specific categories of AI that are presumed to impact rights and safety. The memorandum establishes recommendations for managing risks in federal procurement of AI, including aligning with the law, transparency and performance improvement, promoting competition, maximizing the value of data for AI, and more.

ONC Decision Support Interventions Certification Criteria

Released: January 9, 2024

Background

The Office of the National Coordinator for Health Information Technology (ONC) released the Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing (HTI-1)[6] final rule in December 2023, with provisions becoming effective 30 days after publication in the *Federal Register*. The final rule implements provisions directed by the 21st Century Cures Act and makes enhancements to the ONC Health IT Certification Program. ONC hopes these provisions will advance interoperability, improve transparency, and support the access, exchange, and use of electronic health information.

Contained within the Health IT Certification Program final rule changes is an expansion of the clinician decision support (CDS) criteria requirements renamed decision support interventions (DSI).[7] The requirements on DSI and predictive DSI contained within the HTI-1 final rule mark the first attempt at HHS regulating AI broader than those contained in medical devices and regulated by the FDA. Aimed almost entirely at transparency, the DSI certification criteria will assist those utilizing certified health IT products to understand how DSIs were trained, as well as the data used to train them. Health IT developers are required to update their certified health IT to meet these new requirements by December 31, 2024 and must begin maintaining the ongoing maintenance of certification requirements on January 1, 2025.

Key DSI Requirements

- The addition of 14 new source attributes for predictive DSIs that enable or interface with Health IT Modules providing users with information on what data was used to train the DSI, how the predictive DSI should be used, updated, and maintained, and how the predictive DSI performs using validity and fairness metrics in testing and local data.
    - Those new source attributes require the inclusion of social determinants of health (SDOH) data as well as other health equity data source attributes.
- Incorporates new requirements into the Certification Program for Health IT Modules that support artificial intelligence (AI) and machine learning (ML) technology to increase transparency related to decision support interventions (DSI) created by health IT developers.
- Adds the Clinical Decision Support (CDS) Criterion to the list of applicable certification criteria for real-world testing.
- Requires developers of certified health IT to attest "yes" to an annual review and update of DSI documentation as necessary.

[6] Available at: https://ahima.org//media/k1ilww1y/hti-1-final-rule-ahima-supported-provisions.pdf.
[7] Available at: https://www.healthit.gov/sites/default/files/page/2023-12/HTI-1_DSI_fact%20sheet_508.pdf.

- Requires developers of certified health IT with Health IT Modules certified to attest “yes” or “no” as to whether their Health IT Module is supplied with one or more predictive DSIs.

Areas of Focus for DSI Requirements

- Details and output of the DSI;
- Purpose of the intervention;
- Cautioned out-of-scope use of the intervention;
- Intervention development details and input features;
- Process used to ensure fairness in development of the intervention;
- External validation process;
- Quantitative measures of performance;
- Ongoing maintenance of intervention implementation and use; and
- Updates and continued validation or fairness assessment schedule.

Transparency and Efficacy in DSI

As stated above, one of the requirements within the DSI criterion is that certified health IT must support 13 source attributes for evidence based DSIs and 31 source attributes for predictive DSIs. ONC’s intent is for these attributes to be used to create an industry standard floor of data utilized in the creation and use of DSI. By creating this floor, it will be possible for certified health IT that utilize DSIs to create tools like “advanced structured model cards.” [8]

The source attributes will also be used to assist organizations in the evaluation of Predictive DSIs to determine if they are fair, appropriate, valid, effective, and safe (FAVES). The FAVES methodology outlined by ONC helps determine a Predictive DSI’s quality and whether the information or recommendations it outputs can be trusted for use. ONC recommends organizations utilize the FAVES methodology when possible, in evaluating their implemented DSIs to ensure predictability and trust.

[8] https://www.healthit.gov/sites/default/files/page/2024-01/DSI_HTI1%20Final%20Rule%20Presentation_508.pdf.

HHS Nondiscrimination in Health Program and Activities Proposed Rule

Released: August 4, 2024

Background

The Affordable Care Act (ACA) included protections for patients from discrimination in the healthcare system. These protections are included in Section 1557 and specifically prohibit "discrimination on the basis of race, color, national origin, sex, age, or disability in certain health programs or activities."[9] HHS began an effort in 2022 to update Section 1557 and the nondiscrimination provisions in Centers for Medicare & Medicaid Services (CMS) regulations through proposed rulemaking.

Published on August 4, 2022, the Nondiscrimination in Health Programs and Activities proposed rule[10] contained several provisions that update the regulation to reflect the realities of healthcare operations. The final rule was released on May 6, 2024 as a joint effort by CMS and the HHS Office for Civil Rights (OCR). Included in the proposed changes was a set of nondiscrimination requirements related to the application of clinical algorithms. The final rule states clinical algorithms "are tools used to guide healthcare decision making and can range in form from flowcharts and clinical guidelines to complex computer algorithms, decision support interventions, and models . . . clinical algorithms are used for screening, risk prediction, diagnosis, prognosis, clinical decision making, treatment planning, health care operations, and allocation of resources, all of which affect the care that individuals receive."

Key Provisions

- A covered entity must not discriminate against any individual on the basis of race, color, national origin, sex, age, or disability through the use of clinical algorithms in decision-making.
- Covered entities are not liable for clinical algorithms they did not develop, but may be held liable under this provision for their decisions made in reliance on biased clinical algorithms.
- Covered entities using clinical algorithms in their decision-making should consider clinical algorithms as a tool that supplements their decision-making, rather than as a replacement of their clinical judgement.
- If OCR receives a complaint alleging discrimination resulting from the use of a clinical algorithm in decision making against a covered entity, it will conduct a fact-specific analysis of the allegation. During the investigation, OCR will consider what decisions and actions were taken by the covered entity in reliance of a clinical algorithm in its decision making, and what measures the covered entity took to ensure that its decision and actions resulting from using a clinical algorithm were not discriminatory.

[9] Available at: https://www.hhs.gov/civil-rights/for-providers/laws-regulations-guidance/regulatory-initiatives/1557-fact-sheet/index.html.

[10] Available at: https://www.federalregister.gov/documents/2022/08/04/2022-16217/nondiscrimination-in-health-programs-and-activities.

NIST Artificial Intelligence Risk Management Framework

Released: January 9, 2024

Background

The Artificial Intelligence Risk Management Framework (AI RMF 1.0)[11] is a guidance document developed by the National Institutes for Standards and Technology (NIST) for use by organizations designing, developing, deploying, or using an AI system to help manage the risk included in AI technologies. Congress directed NIST to create a voluntary AI RMF in collaboration with the private and public sectors. The intended audience for the AI RMF is all organizations across different industry sectors so the benefits of AI can be realized with protection from the potential harms.

The AI RMF looks both at AI systems as a whole and specifically at those deployed within organizations. Part one of the AI RMF focuses on the overall risks that come with AI and provides characteristics of trustworthy AI systems. Part two of the AI RMF, what NIST refers to as the core of the framework, outlines how organizations can address risks in AI systems through governance, mapping, measurement, and management.

Key Provisions

The AI RMF refers to AI systems that are engineered or machine-based systems that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments. In the context of those AI systems, the framing of risk for the AI RMF is grounded in minimizing potential negative impacts of AI systems, such as threats to civil liberties and rights, while providing opportunities to maximize positive impact. NIST identifies the following characteristics of a trustworthy AI system:

- Valid and reliable;
- Safe, secure, and resilient;
- Accountable and transparent;
- Explainable and interpretable;
- Privacy-enhanced; and
- Fair with harmful bias managed.

[11] Available at: https://www.nist.gov/news-events/news/2023/01/nist-risk-management-framework-aims-improve-trustworthiness-artificial.

NIST expects that organizations that utilize the AI RMF will benefit from:

- Enhanced processes for governing, mapping, measuring, and managing AI risk, and clearly documenting outcomes;
- Improved awareness of the relationships and tradeoffs among trustworthiness characteristics, socio-technical approaches, and AI risks;
- Explicit processes for making go/no-go system commissioning and deployment decisions;
- Established policies, processes, practices, and procedures for improving organizational accountability efforts related to AI system risks;
- Enhanced organizational culture which prioritizes the identification and management of AI system risks and potential impacts to individuals, communities, organizations, and society;
- Better information sharing within and across organizations about risks, decision-making processes, responsibilities, common pitfalls, and approaches for continuous improvement;
- Greater contextual knowledge for increased awareness of downstream risks; and
- Strengthened engagement with interested parties and relevant AI actors.

NIST details that risk management should be continuous, timely, and performed throughout the AI system lifecycle. The core of those risk management practices should be grounded in governance and feature mapping, measurement, and management of the culture surrounding the AI and the AI system itself. Each of the “cores” — governance, mapping, measurement, and management — include a robust of list of categories and subcategories for each function. These categories and subcategories, when implemented by an organization, encompass the full AI RMF itself.

Deploying AI Systems Securely: Best Practices for Deploying Secure and Resilient AI Systems

Released: April 15, 2024

Background

The National Security Agency's Artificial Intelligence Security Center (NSA AISC) published a joint information sheet in collaboration with the Cybersecurity and Infrastructure Security Administration (CISA), the FBI, and security agencies from Australia, New Zealand, Canada, and the United Kingdom outlining how best to deploy AI systems securely.[12] Contained within the information sheet is guidance on best practices for deploying and operating externally developed AI systems.

Key aims of the guidance include:
- Improving the confidentiality, integrity, and availability of AI systems;
- Ensuring there are appropriate mitigations for known vulnerabilities in AI systems; and
- Providing methodologies and controls to protect, detect, and respond to malicious activity against AI systems and related data and services.

Best practices in the information sheet relate to ML-based AI systems and is geared towards organizations that have implemented externally developed AI systems.

Recommended Best Practices

The information sheet includes the following recommended best practices:
- Securing the deployment environment;
- Determine if existing IT infrastructure where the AI is being deployed applies sound security principles;
- Actively manage deployment environment governance in both the IT system and deployment environment;
- Ensure a robust deployment environment architecture is in place;
- Harden deployment environment configurations; and
- Protect deployment networks from threats.

Continuously protect the AI system:
- Validate the AI system before and during use;
- Secure exposed APIs;
- Actively monitor model behavior; and
- Protect model weights.

[12] Available at: https://media.defense.gov/2024/Apr/15/2003439257/-1/-1/0/CSI-DEPLOYING-AI-SYSTEMS-SECURELY.PDF.

Secure AI operation and maintenance:

- Enforce strict access controls;
- Ensure user awareness and training;
- Conduct audits and penetration testing;
- Implement robust logging and monitoring;
- Update and patch systems regularly;
- Prepare for high availability and disaster recovery; and
- Plan secure delete capabilities.

FDA: Artificial Intelligence & Medical Products

Released: March 15, 2024

Background

The Food and Drug Administration (FDA) is tasked with reviewing medical devices for approval and use within healthcare. Three of the main avenues the FDA utilizes to review and approve medical devices is premarket 510k clearance, De Novo classification, and premarket approval. Approval authorities also include the ability for the FDA to review and clear modifications to medical devices, including software as a medical device.

Currently, the FDA has stated it does not believe the current paradigm of medical device regulation was designed for adaptive artificial intelligence and machine learning technologies.[13] The FDA has stated the Center for Biologics Evaluation and Research (CBER), Center for Drug Evaluation and Research (CDER), Center for Devices and Radiological Health (CDRH), and Office of Combination Products (OCP) within the FDA are working in tandem on a review and approval framework that encompasses AI innovations. As part of the FDA's efforts to clarify how they are approaching AI oversight through their existing authority, the agency released a paper titled, "Artificial Intelligence and Medical Products: How CBER, CDER, CDRH, and OCP are Working Together" detailing how the agency will "collaborate to protect public health while fostering responsible and ethical medical product innovation through AI."

Overview

The paper describes four areas of focus for CBER, CDER, CDRH, and OCP when it comes to evaluating AI within medical products. The areas of focus include:

- Fostering collaboration to safeguard public health;
- Advancing the development of regulatory approaches that support innovation;
- Promoting the development of harmonized standards, guidelines, best practices, and tools; and
- Supporting research related to the evaluation and monitoring of AI performance.

One of the key aims of the FDA is to build regulatory approaches that can be applied across different types of products the FDA reviews. With the FDA limited in its regulatory authority to fully regulate AI, the agency has outlined several actions organized around the four focus areas. These actions include:

- Fostering collaboration to safeguard public health through continued work with developers, patient groups, academia, global regulations, and other interested parties;

[13] https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device.

- Advancing the development of predictable and clear regulatory approaches that support innovation in the use of AI;
- Promoting the development of standards, guidelines, best practices, and tools for the medical product lifecycle that build on Good Machine Learning Practice Guiding Principles[14]; and
- Supporting research related to the evaluation and monitoring of AI performance through demonstration projects and activities that gain insight into AI's impact on medical product safety and effectiveness.

The FDA has reiterated its commitment to working through its regulatory pathways to ensure AI under the agency's purview complies with existing standards. Like many HHS agencies, the paper highlights the FDA's interest in the development and use of standards in AI development and indicates the FDA will continue to adjust its approach to the rapid development of AI and the continual need for regulatory adjustments.

[14] Available at: https://www.fda.gov/medical-devices/software-medical-device-samd/good-machine-learning-practice-medical-device-development-guiding-principles.