DEPARTMENT: Ethics and Compliance	**POLICY DESCRIPTION:** Responsible AI
PAGE: 1 of 8	**REPLACES POLICY DATED:**
EFFECTIVE DATE: October 1, 2024	**REFERENCE NUMBER:** EC.031
APPROVED BY: Ethics and Compliance Policy Committee	

SCOPE: All HCA Healthcare ("Company") affiliated facilities worldwide including, but not limited to, hospitals, ambulatory surgery centers, home health centers, home health agencies, hospice agencies, physician practices, outpatient imaging centers, urgent care centers, Parallon, joint ventures and all Corporate Departments, Groups, Divisions, and Markets (collectively, "Affiliated Employers" and individually, "Affiliated Employer").

PURPOSE: To ensure the responsible development, deployment, and use of Artificial Intelligence ("AI") across the Company following the pillars of the Responsible AI Framework as outlined in the Company's Code of Conduct ("Code"). Responsible AI includes respecting individuals' privacy, promoting transparency, fairness, bias minimization, accountability, and operation in a safe and secure manner that strives to protect individuals from physical, emotional, environmental, and/or digital harm.

POLICY: This policy applies to: employees', contractors', service providers', and/or vendors' (collectively, "Colleagues") use, engagement, development, or interaction with Company-owned, externally purchased, or publicly available AI Solutions; the data used, stored, and processed for training AI models, and any other tools instrumental in creating Outputs; and AI Solutions in any and all forms, including, without limitation, AI Solutions that are standardized, custom-developed, stand-alone, or bundled with or embedded into any product or service.

1. **Acceptable Use**

   The use of AI Solutions is solely for tasks that contribute directly to Company business objectives and duties and in alignment with the Code, applicable policies, procedures, and law. Colleagues are only allowed to use AI Solutions and tools approved by the Company.

2. **Prohibited Use**

   The Company has identified two specific uses of AI Solutions that are prohibited as a matter of Company policy.

   a. *Dark Patterns*. AI Solutions may not be used to distort, impair, trick, or otherwise interfere with the ability of an individual to make autonomous and informed choices or decisions, or otherwise manipulate a person through subliminal techniques, or so-called dark patterns, to make (or not make) a particular decision or take/refrain from a particular action.

   b. *Exploiting Vulnerabilities*. AI Solutions may not be used to exploit potential vulnerabilities of an individual or to distort or impair their ability to make autonomous and informed choices or decisions or otherwise manipulate or cause physical or psychological harm to themselves or others.

3. **Responsible AI Governance Council**

   The Responsible AI ("RAI") Governance Council has been established to address areas of stakeholder engagement, ethical considerations, policy development, risk management, and compliance aspects pertaining to AI Solutions.

4. **Notifications and Reporting**

When using an approved AI Solution, Colleagues are responsible to:

- Promptly notify the Director of Responsible AI if any of the following are observed: anomalies, a decline or material deviation in accuracy of Outputs, biased, discriminatory, or illegal Outputs, or Outputs that divert from expectations as outlined in the Code or applicable Company policies and procedures or the AI Solutions documentation. The Director of Responsible AI is to report any such occurrence to the RAI Governance Council as appropriate.
- Immediately report any suspected or actual inadvertent disclosure of Company Data to Information Protection and Security.
- Ensure thorough periodic review that the AI Solution continues to be in alignment with the Code and applicable Company policies and procedures.

Colleagues should reference the AI Acceptable Use Guidelines for more details.

PROCEDURE:

1. **Seeking Use of AI Solution**
    a. Those seeking an external solution leveraging AI must follow Company solution submission and approval processes. A RAI Questionnaire will be submitted as a function of the AI Solution submission and approval processes and RAI risk assessment performed.
    b. Those seeking to engage in development, co-development, or deployment of solutions (AI Development Lifecycle) leveraging AI must first contact the Director of Responsible AI prior to initiating any development or deployment.
        i. A Use Case Risk Assessment will be performed during solution ideation.
        ii. A Data Risk Assessment will be performed prior to solution development.
        iii. A Validation Risk Assessment will occur prior to moving to solution production or deployment.
    c. All solutions leveraging AI will be subject to periodic audit for the duration of the solution lifespan until deprecation to ensure compliance and alignment with the RAI framework. Any solution leveraging AI that undergoes an internally or externally initiated or offered upgrade or new version shall be subject to an audit to ensure continued compliance and alignment with the RAI.
    d. Solution approval and review is subject to a risk score and the RAI Governance Council reserves the right to review or rescind approval at any time. Solutions proposed for review before the RAI Governance Council and Steering Committee will be prioritized on risk versus enterprise impact.

i. Low Risk Score: Automatic approval and awareness of the RAI Governance Council.

ii. Medium Risk Score: Review by steering committee, mitigation recommendations, and awareness of RAI Governance Council.

iii. High Risk Score: Review by steering committee, mitigation recommendations, referral to full RAI Governance Council, and issuance of a written go/no-go decision by the RAI Governance Council.

iv. Critical Risk Score: Review by steering committee, mitigation recommendations, referral to full RAI Governance Council, and issuance of a written go/no-go decision by the RAI Governance Council.

e. The Company will maintain a process for creation and maintenance of an AI solution inventory. For further information, contact the Director of Responsible AI.

2. **Quality Control of Outputs**

a. Potential errors in Outputs may occur for a variety of reasons. All Outputs must be verified by reasonable means as identified in the applicable training, documentation, or guidelines for the AI Solution, or, in the absence of identified reasonable means, Users must seek assistance and guidance from the Director of Responsible AI.

b. Before using Outputs, Users must engage in an independent review by taking the following into account:

- Proofreading: Carefully proofread the Output for grammar, spelling, and punctuation errors.
- Edit as Needed: If necessary, make edits to improve clarity, coherence, and overall quality of the Output.
- Engage Human Oversight: Involve human oversight in the final review process. Human oversight of AI Solutions and Outputs serves to identify solution-specific and Output dependent nuances, vulnerabilities, potential shortcomings, and opportunities for continued improvement.

3. **Solution Development and Monitoring**

To ensure responsible development, deployment and monitoring of AI Solutions, Users must abide by the following:

- Complete an intake questionnaire to document the inherent risk associated with the applicable development and deployment, of the solution and to prioritize Responsible AI Program reviews through risk tiers.
- Data usage, storage, disclosure, and destruction must: (i) comply with applicable legal requirements; (ii) comply with all applicable Company policies and procedures; (iii) comply with terms outlined in any applicable agreement relating to or involving the

data; (iv) undergo evaluation for completeness and accuracy; and (v) incorporate controls to protect individuals' privacy and rights (e.g., data minimization practices).

- Document key assumptions and decisions, including any applicable or otherwise appropriate version control, relating to solution design and development.
- Accountable and consistent monitoring of solution performance and Outcome generation.
- Utilize self-regulation (e.g., risk assessment, cloud tools, etc.) to support compliance with applicable legal requirements, industry standards, and applicable Company policies and procedures.

Consult the Responsible AI Development and Monitoring Standard for comprehensive guidelines and requirements around solution development and monitoring.

4. **Cybersecurity and Malicious Use**

a. The use and development of AI Solutions can pose cybersecurity risks to Company systems, devices and infrastructure. To protect Company resources and data and the privacy of other Users, Colleagues, and/or individuals when using or developing AI Solutions, Users must not:

- Develop or deploy Malicious Software.
- Create, distribute, or support creation or distribution of offensive, discriminatory, or illegal content.
- Manipulate or deceive others.
- Violate, infringe, or attempt to violate or infringe the legal and civil rights and liberties of others.
- Infringe, or attempt to infringe, on the intellectual property rights of the Company or others.
- Engage in activity that may violate others' privacy.
- Use or attempt to use the AI Solution to circumvent or attempt to circumvent Company policies or procedures, including but not limited to, Information Protection and Security Policies and Information Security Standards.
- Tamper with Outputs or related processes in AI Solution development or deployment.
- Maliciously prompt or alter the AI Solution, including through prompt injection, prompt obstruction, data dumping, or otherwise engage in any unauthorized modifications that could compromise the integrity of the AI Solution or Outputs.
- Use unauthorized public AI Solutions with Company managed devices, or on/through Company systems, servers, or infrastructure.
- Upload to, or use, any Company Data with an unauthorized public AI Solution.

- Use unauthorized public AI Solutions to generate, revise, or manipulate Outputs for any Company purposes (e.g., software development, communications, decision making, etc.).
- Use or further disseminate for use, any raw Output that has not undergone thorough testing, including but not limited to, vulnerability scanning through enterprise scanning tools, static code analysis, and addressing security issues (including but not limited to OWASP's Top 10).

b. While using or developing AI Solutions, Users shall continually validate and assess the functionality, accuracy, reliability, and security of any Output.

5. **Bias and Discrimination**

AI Solutions may produce biased or discriminatory Outputs. All Users must vigilantly assess Outputs for any such biases, and Outputs must not be used if found or suspected to be biased, misleading, harmful, offensive, or discriminatory. Bias and discrimination should also be assessed across the AI lifecycle and monitored throughout development, deployment, and depreciation.

All Users are responsible for ensuring AI Solutions align with all applicable legal requirements and Company policies and procedures. If any User(s) observes or becomes aware of suspected biased or discriminatory outcomes from Output, such User(s) shall promptly notify the Director of Responsible AI.

6. **Vendor Management**

Only use vendors, contractors, service providers, and/or public AI Solutions as approved by the Application Portfolio Management (APM) Process. If procuring or evaluating a new AI Solution from a third-party vendor, Colleagues must also complete the Vendor Risk Assessment Questionnaire to determine (i) an appropriate risk score; (ii) whether the potential third-party vendor is qualified and approved for use; and (iii) whether the third-party vendor and proposed AI Solution adheres to Responsible AI practices. Any existing product that adds a new AI module, component, or functionality must follow the APM Process for recertification.

The Company expects and requires third-party vendors to commit to responsible development, deployment, and use of AI through a Responsible AI Program. This includes the third-party vendor assessing the AI Solution's performance and compliance, in addition to periodic audits for data privacy and security practices and, as appropriate, bias in the AI Solution.

7. **Training**

Prior to developing, deploying, or using any AI Solution, all Colleagues will complete training and educational programs, as may be designated from time-to-time by the RAI Governance Council, to ensure compliance with the Company's Responsible AI Program and related commitments.

Company-required trainings and educational programs will include, at a minimum:

- New Colleague training modules for Responsible AI;
- Annual refresher training; and

- Personal trainings based on job role, functions, and duties.

Additionally, the RAI Governance Council will approve the scope of an "AI Fundamentals and Best Practices" training program designated for certain Colleagues.

Company and Affiliated Employers will be responsible for designing, implementing, and maintaining training and educational programs specific to AI Technology Activities.

8. **Sanctions**

Violation of this policy may result in disciplinary action, up to and including termination of employment or contract, as well as potential legal and financial penalties. Suspected violations of this policy must be handled in accordance with this policy, the Code, and any applicable Company policies and procedures.

9. **Modifications to Policy**

AI Solutions and the laws and regulations governing AI Solutions are rapidly evolving, and these policies may be amended from time to time to reflect the evolving landscape.

Some jurisdictions have separate laws that may apply additional legal requirements. Consult with legal counsel to identify and comply with any such additional legal mandates.

DEFINITIONS:

AI Development Lifecycle means the iterative process that turns a business problem into an AI Solution through the following four phases: 1) define & initiate; 2) research & design; 3) develop, train, test, & deploy; and 4) operate, monitor, & maintain.

AI Solutions or AI Technology means Artificial Intelligence and Machine Learning technologies both individually and collectively, unless otherwise specified within the context of its use.

AI Technology Activity or **AI Technology Activities** means the acquisition, use, development, deployment, modification, distribution, or otherwise making available by or for the Company of AI Technology.

Artificial Intelligence (AI) means 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 such as patterns and structures learned from existing data, deep learning, neural networks, and machine learning techniques to, among other actions, (1) perceive real and virtual environments; (2) abstract such perceptions into models through analysis in an automated manner; (3) create new, original content, such as images, text, or music; (4) produce content autonomously that closely resembles human-created output; (5) produce natural language texts based on a given input, such as a prompt, a keyword, or a query and/or (6) use model inference to formulate options for information or action.

Company Data means any and all Confidential Information generated, obtained or held by the Company in the course of its operations (whether text, images, code, graphics, video or other

information) in any form, and however stored, transmitted or generated, including, without limitation all archives, derivatives, modifications or manipulations of the foregoing information.

Director of Responsible AI means the Colleague(s) identified by the RAI Governance Council from time to time who is responsible for the management and oversight of the Responsible AI Program.

Machine Learning means an application of Artificial Intelligence that is characterized by providing systems the ability to automatically learn and improve based on Training Materials or experience, without being explicitly programmed.

Malicious Software means any type of code, software, application, or program that is designed to: (1) cause unauthorized access to, theft of, or intrusion upon; or (2) otherwise disrupt, lock, or damage computer equipment, software, networks, infrastructure, or data (commonly referred to as malware, virus, worm, time bomb, ransomware, Trojan horse, or spyware); or (3) software that allows an individual, network, system, or User to bypass normal authentication or authorization functions or other security controls to a product, service, system, network, or other infrastructure or system that would allow the individual, network, system, or User to remain undetected or unaudited.

Output(s) means any outcome, output, or other result, action, or decision obtained from or otherwise performed by or with the assistance of, an AI Technology and/or AI Solution.

Responsible AI means the area of AI governance that applies across all AI Technology Activities and establishes guidelines to address safety and security, trustworthiness, transparency, fairness, and ethics.

Responsible AI (RAI) Governance Council means the Sponsors, Steering Committee, and Advisory Committee as confirmed from time-to-time within the Company who provide sponsorship of the Responsible AI Program and focus on impacts to the enterprise, funding, timeline, and major risks arising from AI Technology Activities.

Responsible AI Framework means the Responsible AI governance framework that documents how Company addresses Responsible AI.

Responsible AI Program means Company's program that oversees and administers Responsible AI and is designed to harmonize ethical considerations, technical advancements, regulatory adherence, and innovation through AI Solutions.

Training Materials means the information (e.g., personal information, personally identifiable information, facts, and other non-copyrightable information), raw data (e.g., metadata, sensor data), content (e.g., licensed or unlicensed, public domain), and other input that is used to train or otherwise develop an AI Technology and/or AI Solution.

Users means Colleagues, developers, subcontractors, and other professionals using, developing, or deploying AI Solutions.

DEPARTMENT: Ethics and Compliance	**POLICY DESCRIPTION:** Responsible AI
PAGE: 8 of 8	**REPLACES POLICY DATED:**
EFFECTIVE DATE: October 1, 2024	**REFERENCE NUMBER:** EC.031
APPROVED BY: Ethics and Compliance Policy Committee	

REFERENCES:

1. Company Code of Conduct
2. Responsible AI Development and Monitoring Standard
3. AI Acceptable Use Guidelines
4. AI Fundamentals and Best Practices
5. Application Portfolio Management (APM) Process
6. Vendor Risk Assessment Questionnaire
7. Responsible AI Questionnaire
8. Use Case Risk Assessment
9. Data Risk Assessment
10. Validation Risk Assessment
11. Third Party Assessment Governance Process
12. Patient Privacy Program Requirements Policy, IP.PRI.001
13. Information Protection & Security
14. Responsible Use of Generative Artificial Intelligence In Scholarly Work, COG.PUB.003
15. Protecting and Mitigating Inappropriate or Unauthorized Access, Use and/or Disclosure of Personally Identifiable Information (PII), IP.GEN.002
16. Release of Company Data to External Entities, IP.GEN.004
17. Global Privacy Policy – General Data Protection Regulation, IP.GEN.005
18. Authorization for Uses and Disclosures of Protected Health Information, IP.PRI.010
19. Minimum Necessary, IP.PRI.003
20. Information Confidentiality and Security Agreements, IP.SEC.005
21. Copyright, LL.GEN.002
22. PC Software License Management (Formerly IP.SEC.003), LL.IP.002

The Responsible AI policy, EC.031, is being released for awareness with an October 1, 2024 effective date. Education and supporting documents associated with this policy are currently being developed and expected to be made available by the policy's effective date. In addition, a review of multiple existing policies is occurring to determine if revisions are necessary related to the use, development and deployment of AI. If you have any questions regarding this policy, please contact CORPResponsibleAI@HCAHealthcare.com.