



Origination 8/26/2025
Last Approved 6/4/2026
Effective 6/16/2026
Last Revised 6/4/2026
Next Review 6/3/2029

Owner Ronald Fuschillo:
Executive Owner
Area Information Technology
References Smith, Louis

Artificial Intelligence (AI)_4615

PURPOSE:

To outline the principles and guidelines to ethically, compliantly, and effectively deploy and use artificial intelligence (AI) systems as supportive tools to meet Harris Health's goals. This policy ensures that AI systems are deployed and used in ways that uphold the highest levels of safety, confidentiality, integrity, and availability of all data and information systems with AI capabilities.

POLICY STATEMENT:

Harris Health supports the responsible and innovative deployment and use of AI Systems to enhance healthcare delivery and improve operational efficiency. All AI Systems must prioritize the secure, legal, and ethical deployment and use of Harris Health data and information systems in a manner that upholds the highest standards of care.

This policy applies to all AI Systems approved for deployment and use at Harris Health, including AI Systems procured from third-party vendors, deployed by Harris Health, embedded in software approved for use at Harris Health (e.g. Microsoft, ServiceNow, Epic), and/or used by third-parties to do work for Harris Health.

POLICY ELABORATION:

I. DEFINITIONS

- A. **Artificial Intelligence (AI) System:** A tool that uses machine learning, natural language processing, deep learning, and/or related technologies to support Harris Health operations. AI Systems process large data sets to make decisions, predictions, recommendations, or generate communications.

Note: Texas law defines AI System as "A machine-based system that infers from inputs how to generate outputs, such as decisions, predictions or recommendations, that influence physical or

digital environments." Harris Health interprets this definition as stated above.

- B. **Availability:** Ensuring that Data and Information Systems are accessible and useable upon demand by an authorized workforce member.
- C. **Bias in AI Systems:** The systematic tendency of an AI System to produce outputs that unfairly favor or disadvantage certain individuals or groups based on attributes such as race, gender, age, language, or socioeconomic status. This bias can emerge from the large data sets used to train the AI System's model, the design of the AI System's algorithm, or the way the AI System's model is prompted and deployed.
- D. **Confidentiality:** The protection from unauthorized use or disclosure of any confidential or sensitive data or information. This includes Protected Health Information.
- E. **Confidential Information:** Information that has been deemed or designated confidential by law (i.e., constitutional, statutory, regulatory, or judicial decision).
- F. **Data:** Any information, structured or unstructured, that is collected, maintained, processed, or analyzed.
- G. **Deployer:** A person or entity that uses an AI System. Harris Health is a Deployer.
- H. **Developer:** A person or entity that creates an AI System for sale, lease, or distribution in Texas. Harris Health is not currently a Developer.
- I. **Information Owner:** An individual who has responsibility for controlling the production, development, change, maintenance, access, use, resiliency, and security of the Data or Information System or a component thereof.
- J. **Information System:** Any telecommunications and/or computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data (digital or analog); it includes software, firmware, and hardware. This definition also includes subsidized devices.
- K. **Integrity:** Ensuring that data or information has not been altered or destroyed in an unauthorized manner.
- L. **Protected Health Information (PHI):** Individually identifiable health information that is created, received, transmitted, or maintained by Harris Health in any form or medium that relates to the patient's healthcare condition, provision of healthcare, or payment for the provision of healthcare, as further defined in the HIPAA regulations. PHI includes, but is not limited to, the following identifiers:
 - 1. Name;
 - 2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to current publicly available data from the Bureau of the Census:
 - a. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
 - b. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
 - 3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

4. Telephone numbers;
 5. Fax numbers;
 6. Electronic mail addresses;
 7. Social Security numbers;
 8. Medical record numbers;
 9. Health plan beneficiary numbers;
 10. Account numbers;
 11. Certificate/license numbers;
 12. Vehicle identifiers and serial numbers, including license plate numbers;
 13. Device identifiers and serial numbers;
 14. Web Universal Resource Locators (URLs);
 15. Internet Protocol (IP) address numbers;
 16. Biometric identifiers, including finger and voice prints;
 17. Full face photographic images and any comparable images; and
 18. Any other unique identifying number, characteristic, or code, except permitted for re-identification purposes.
- M. **Safety:** A measurement of an Information System's ability to avoid unwanted harm, loss, injury, or damage.
- N. **Workforce:** Harris Health Board of Trustees, employees, medical staff, trainees, contractors, volunteers, and vendors.

II. AI Governance Committee

Harris Health's AI Governance Committee is responsible for overseeing Harris Health's AI Program to ensure the appropriate, secure, and regulated deployment and use of AI System(s) at Harris Health to enable the enterprise to achieve its strategy and goals. The committee's actions will support the provisions set forth in this policy.

The AI Governance Committee's Charter outlines the duties, scope, and authority of the committee.

III. General Principles

The following are general principles for AI deployment and use at Harris Health:

- A. **Accuracy and Reliability:** Workforce members must verify information provided by AI Systems for accuracy and reliability before making decisions, taking action, or sharing the information. Workforce members must not use information provided by AI Systems if the Workforce member determines doing so will cause harm to patients or others.

AI Systems should complement human expertise rather than replace human judgment. AI Systems rely on sources with varying degrees of quality and reliability. Information from AI Systems is generated based on patterns and probabilities rather than personal knowledge or critical thinking.

- B. **Bias Mitigation:** AI Systems must undergo periodic reviews for biases, ensuring fair and unbiased

healthcare for all demographics. AI Systems must be tested across various patient populations to prevent unintended disparities. These reviews will include an evaluation of incidents reported by Workforce members. The results of these reviews will be reported to the AI Governance Committee and mitigating strategies will be developed and implemented as necessary.

- C. **Patient Privacy and Data Security:** Workforce members must only use AI Systems approved for use by Harris Health to perform job duties. Effective January 5, 2026, unapproved AI Systems will be blocked for use from Harris Health devices and must not be used on your personal device to perform Harris Health job duties.
- D. **Responsible and Ethical Use:** AI Systems must be used responsibly, ethically, and in compliance with Harris Health policies, including Harris Health's Code of Conduct, as well as the Texas AI Code of Ethics, once available. Workforce members must be aware that AI Systems may generate potentially biased outputs. Workforce members are prohibited from using AI to generate or disseminate content that is discriminatory, offensive, or violates Harris Health policies or procedures.
- E. **Recognizing Limitations:** AI Systems are tools to support, not replace, human oversight and AI is not a substitute for professional and/or clinical expertise or judgment. For example, AI Systems may struggle with understanding nuanced or complex information, or medical scenarios.
- F. **Continuous Learning and Improvement:** AI Systems can serve as a general learning tool, but it must not replace professional development and formal training related to a Workforce member's role and workplace responsibilities.
- G. **Reporting and Accountability:** Harris Health has established clear channels for reporting potential misuse or concerns about AI Systems. If you encounter any issues, please report them immediately to the IT Service Desk. Harris Health takes all reports seriously to ensure responsible and ethical use of AI Systems. The AI Governance Committee will review data from these reports periodically and incorporate findings into system updates and policy revisions.

IV. Requirements

The following are requirements for AI deployment and use at Harris Health:

- A. All AI Systems must undergo review for approval through Harris Health's Technology Governance framework, which includes approval by the AI Governance Committee, prior to deployment or use. This includes AI Systems used by Harris Health vendors to perform work for Harris Health. As a part of this process, the Information Security Risk Assessment (ISRA) must be completed to evaluate potential risks related to data security, privacy, and system integrity. For more information, refer to Harris Health Policy 3.11.804, Information Security Risk Assessment.
- B. A list of all AI Systems approved for deployment and use at Harris Health will be maintained and made available to Harris Health Workforce members. This list will include a detailed description of each AI System, including information about the AI System's classification, decision-making process(es), methods for information generation, intended use, and what Data the AI System will have access to.
- C. Workforce members must acknowledge this policy and complete a designated education module prior to being granted access to AI Systems.
- D. AI Systems use must comply with all applicable laws, regulations, and Harris Health policies and procedures, as well as the Texas Department of Information Resources Code of Ethics Government Code 2054.702.
- E. AI Systems must be restricted to only the Data and functions necessary to perform the desired

operations in accordance with Harris Health's Global Data Classification Policy.

F. Required regulatory reporting regarding AI must be completed in compliance with state law.

V. Risks and Prohibited Actions:

Harris Health acknowledges that AI Systems present risk. These risks include, but are not limited to: (1) safety; (2) confidentiality; (3) integrity; (4) bias and discrimination; and (5) ethical and legal/regulatory risk, including copyright/intellectual property. To mitigate against these risks, Harris Health prohibits the following related to AI use by Workforce members:

- A. **Unauthorized Access:** Accessing AI systems or data without proper authorization; using unapproved AI Systems from personal devices to perform work-related functions.
- B. **Data Manipulation:** Altering or falsifying data used by AI systems. Examples include uploading inaccurate or false data into AI systems, directing AI systems to look at known inaccurate or false data, or not reasonably validating data used by AI systems is accurate.
- C. **Privacy Violations:** Intentionally or unintentionally using AI to access, use, or disclose sensitive or Confidential Information without proper authorization. The following prohibition and acceptable use provisions apply specifically to Copilot:
 - 1. Workforce members with a Copilot Enterprise License (i.e., Access to Copilot's Work and Web tab):
 - a. Workforce members are PROHIBITED from using sensitive or Confidential Information, including PHI, in Copilot prompts on the WEB tab.
 - b. Workforce members MAY USE Confidential Information or sensitive information, including PHI, in Copilot prompts on the WORK tab as the data remains within the Harris Health tenant (only Workforce members with a Copilot Enterprise License have access to the Work tab).
 - 2. Any use of Confidential Information or sensitive information, including PHI, in Copilot prompts must comply with all applicable Harris Health policies, and must be (1) necessary to perform the Workforce member's job duties; and (2) be limited to the minimum amount of information necessary to perform the Workforce member's job duties.
 - 3. Workforce members without a Copilot Enterprise License (i.e. No access to Copilot's Work tab):

Workforce members are PROHIBITED from using Confidential Information or sensitive information, including PHI in Copilot prompts.
 - 4. See Appendix A for a Quick Reference Guide on this topic.
- D. **Bias and Discrimination:** The deployment or approval of information from AI systems that exhibit bias or discrimination against any group of individuals.
- E. **Unethical Use:** Using AI for purposes that are unethical or not aligned with Harris Health's policies and procedures, including the Texas Department of Information Resources Code of Ethics Government Code 2054.702. Examples include: using AI to create or distribute offensive, discriminatory, or illegal content; using AI to manipulate or deceive others; or infringing or attempting to infringe upon the intellectual property rights of Harris Health or others.
- F. **Neglecting Human Oversight:** Relying solely on AI for critical decision-making without human

oversight.

- G. **Cyber/Information Security/Privacy Breaches:** Failing to implement adequate measures to protect Data from breaches; using AI Systems not approved for use by Harris Health to perform your job duties.
- H. **Development of AI System:** Developing, training, fine-tuning, prompt-engineering, testing, or deploying any unapproved AI system (including use of external generative-AI tools) with Harris Health data, systems, brand, or patient/workforce interactions without prior written approval from the AI Governance Committee. Harris Health is not currently a Developer of AI Systems.

REFERENCES/BIBLIOGRAPHY:

Texas Department of Information Resources Code of Ethics Government Code 2054.702.

Chapters 551 and 552, Texas Business & Commerce Code

Harris Health Policy 6.37, Acceptable Use of Harris Health Information Systems

Harris Health Policy 3.11.804, Information Security Risk Assessment

Artificial Intelligence Risk Management Framework (AI RMF 1.0); National Institute of Standards and Technology, U.S. Department of Commerce; [AI Risk Management Framework | NIST](#)

Augmented Intelligence Development, Deployment, and Use in Health Care; American Medical Association, [AMA Principles for Augmented Intelligence Development, Deployment, and Use](#)

OFFICE OF PRIMARY RESPONSIBILITY:

Information Technology

APPENDIX A:

CoPilot Quick Reference Guide

COPY

Copilot – Web Tab vs. Work Tab

This guide explains how to use the Microsoft Copilot Web tab and Work tab safely.

The target audience for this guide is all Harris Health workforce members who have access to Microsoft Copilot.

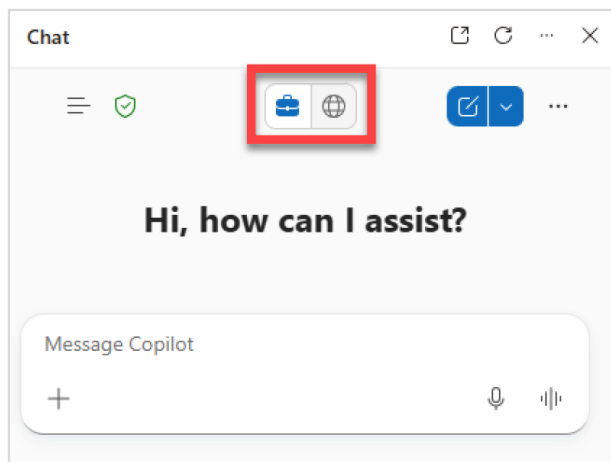
Table of Contents

Overview	1
Key Definitions	2
At-a-Glance: Web Tab vs Work Tab	2
Decision Tree: Should I Put This into Copilot?	4
Real-World Examples	5
Frequently Asked Questions	5
Who to Contact	6

Overview

How to use the Copilot Web tab and Work tab safely:

- When using the Copilot **Web** tab, you should never include confidential or sensitive information, including PHI.
- When using the Copilot **Work** tab, you may use confidential information but only share what you need to perform your job.



HARRISHEALTH

ITEDUCATION
Microsoft Copilot



June 8, 2026
Page 1
RM

Copilot – Web Tab vs. Work Tab

Key Definitions

- **Copilot:** Microsoft's generative AI assistant. Copilot has two surfaces inside Harris Health: a public Web tab and an enterprise Work tab.
- **Web tab:** The general internet side of Copilot. Prompts and responses may leave the Harris Health environment and are governed by Microsoft's consumer terms.
- **Work tab:** The enterprise side of Copilot. Prompts and responses stay inside the Harris Health tenant. Only workforce members with the Copilot Enterprise License can access the Work tab.
- **Confidential or sensitive information:** Any non-public information, including but not limited to PHI, PII, financial data, credentials, internal policies, contracts, legal documents, and network or security configurations. Please refer to the [Harris Health Artificial Intelligence \(AI\) Policy](#) for the full definition.
- **PHI (Protected Health Information):** Health information that can be tied to a specific patient, including but not limited to names, MRNs, dates of birth, diagnoses, treatment notes, and photos. Please refer to the [Harris Health Artificial Intelligence \(AI\) Policy](#) for the full definition.
- **Minimum necessary:** A HIPAA principle. Use only the smallest amount of information needed to complete the task. If you do not need it, do not include it. Please refer to the [Harris Health Minimum Necessary Standard for Request, Use or Disclosure of Protected Health Information Policy](#) for the full definition.

At-a-Glance: Web Tab vs. Work Tab

Use this table when you need a quick side-by-side reminder of how each tab is used.

ASK YOURSELF	WEB TAB	WORK TAB
Where does my data go?	Outside Harris Health; processed and may be retained by Microsoft under consumer terms.	Stays inside the Harris Health tenant.
Who has access?	Anyone on the internet using Copilot.	Only workforce members with the Copilot Enterprise License.
Can I include PHI?	No. Never.	Yes, when it is needed for your job and is the minimum necessary.

HARRISHEALTH

ITEDUCATION
Microsoft Copilot



June 8, 2026
Page 2
RM

Copilot – Web Tab vs. Work Tab

ASK YOURSELF	WEB TAB	WORK TAB
Can I include other sensitive info? (financial data, credentials, internal policy, legal documents)	No.	Yes, with the same job-need and minimum-necessary tests.
Best used for	Public information, general drafting, research that does not involve Harris Health data.	Harris Health workflow tasks that need patient or internal data.
Example safe prompt	Explain HIPAA's minimum necessary standard in plain language.	Summarize this clinical note for the patient I am seeing today.

Quick tip: If you are about to paste anything that contains a patient name, MRN, chart number, internal Harris Health document text, credentials, or any other information you would not post on a public website, do not use the Web tab. Switch to Work, or remove the sensitive information first.

HARRISHEALTH

ITEDUCATION
Microsoft Copilot



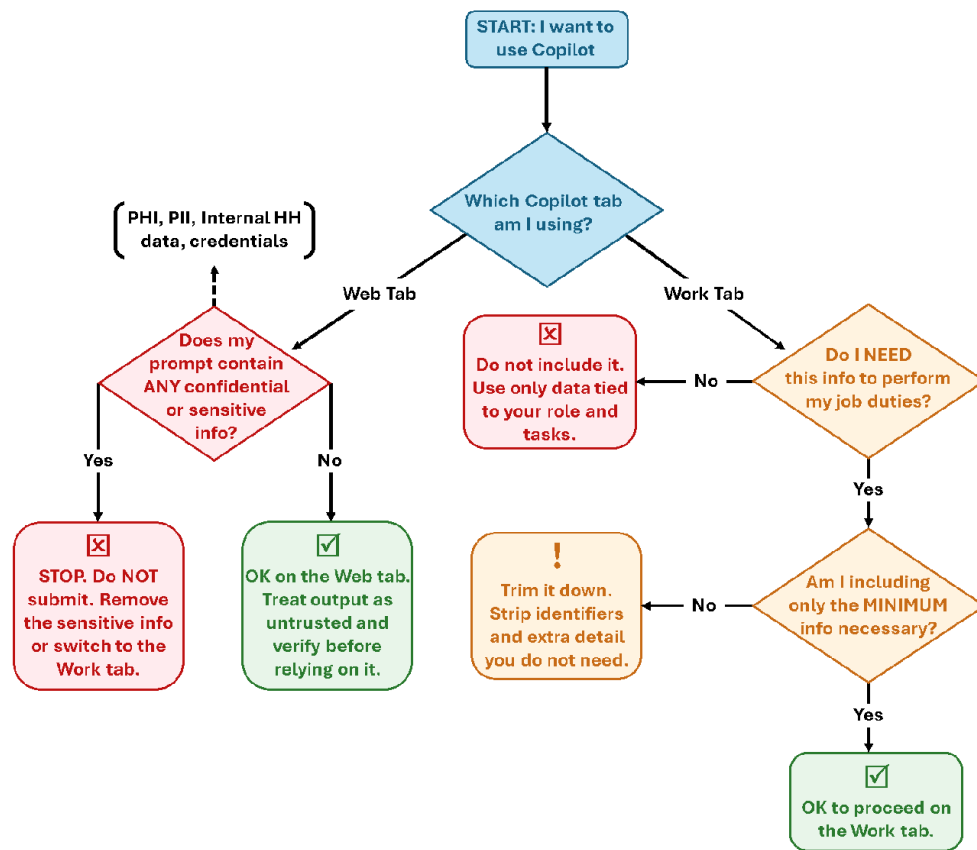
June 8, 2026
Page 3
RM

Copilot – Web Tab vs. Work Tab

Decision Tree: Should I Put This into Copilot?

Walk through this flow chart whenever you are unsure about what to put into Copilot. The same logic applies for any prompt, attachment, or pasted content.

Note: When the answer is still unclear, pause and contact Compliance before submitting.



Copilot – Web Tab vs. Work Tab

Real-World Examples

Examples are illustrative. The principle is what matters: keep confidential info off the Web tab, and on the Work tab use only what you need for your job.

WEB TAB examples	WORK TAB examples
On the Web tab, NEVER include confidential or sensitive info. ✓ Explain HIPAA's minimum necessary standard in plain language. ✓ Suggest agenda items for a generic project kickoff meeting. ✓ Summarize current best practices for hospital wayfinding signage. ✗ Draft a discharge summary for Jane Doe, MRN 12345, admitted for pneumonia. (PHI) ✗ Review this internal Harris Health policy on incident response. (Confidential) ✗ Help me write a performance plan for [employee name]. (PII and confidential) ✗ Here is our network diagram, suggest improvements. (Security config)	On the Work tab, confidential info is allowed, but only what you need. ✓ Summarize this clinical note for the patient I am rounding on. ✓ Draft a response to this patient complaint email I received. ✓ Build a project plan for our Epic optimization initiative. ✓ Compare these two internal vendor proposals and highlight differences. ! Think twice: "Pull every patient with diagnosis X." Is that minimum necessary for your job? ✗ Show me a coworker's medical record. (Not a job duty) ✗ Summarize all open compliance investigations. (Not minimum necessary unless that is your role)

Frequently Asked Questions

Q: How do I tell which tab I am on?

A: Look at the tab indicator at the top of the Copilot window. The Work tab shows your Harris Health identity and an enterprise indicator. If you are unsure, stop and verify before pasting anything sensitive.

Q: What if I accidentally entered PHI or other sensitive info on the Web tab?

A: Do not try to delete it yourself. Stop using the prompt, take a screenshot if you safely can, and contact the Information Security team right away. The team will work with Compliance to assess and handle the incident.

HARRISHEALTH

IT EDUCATION
Microsoft Copilot



June 8, 2026
Page 5
RM

Copilot – Web Tab vs. Work Tab

Q: Can I copy a Copilot response from the Web tab into a clinical note or business document?

A: Treat Web tab output as draft and unverified. Anything used in a clinical or business decision must be reviewed and verified by a qualified human. Never paste Web tab output directly into the medical record.

Q: What about other AI tools? ChatGPT, Gemini, public Claude, free apps?

A: Same rule. If it is not the enterprise-licensed Work tab inside Harris Health, treat it as the public internet. Do not enter Harris Health confidential information into it.

Q: I am unsure whether something is "minimum necessary." How do I decide?

A: Use your professional judgment and lean toward less. Ask: would my job still get done if I left this detail out? If yes, leave it out. When in doubt, your manager or Compliance can help.

Q: Does this apply to attachments and uploaded files too?

A: Yes. The same rules apply whether you type the info, paste it, or upload a document. A scanned chart or an exported spreadsheet of PHI does not belong on the Web tab.

Who to Contact

Information Security: InfoSec@harrishealth.org

Compliance: Compliance@harrishealth.org

IT Service Desk: Service Desk portal or extension as listed on the intranet

Copyright Notice and General Disclaimer: Information presented in this guide is subject to copyright protection and is intended only for internal use. Data used is PHI-free but should remain confidential.

HARRISHEALTH

ITEducation
Microsoft Copilot



June 8, 2026
Page 6
RM

Attachments

 [CoPilot - Quick Reference Guide \(QRG\) pdf](#)

Approval Signatures

Step Description	Approver	Date
Publisher Approval	Eileen Tseng Stultz	6/16/2026
Policy SOS Committee	Lauren Banks: Executive Owner	6/15/2026
Policy Owner	Ronald Fuschillo: Executive Owner [LB]	6/15/2026
Workflow Start Notification	Lauren Banks: Executive Owner	5/28/2026

COPY