LeadingAge® Ohio

AI Toolkit

CONSIDERATIONS FOR THE GROWING WORLD OF ARTIFICIAL INTELLIGENCE

Includes:

- What is AI?
- Key Terms
- AI Risk Tolerance
- AI + HIPAA
- Sample Policies

Artificial Intelligence (AI) tools are moving quickly into everyday operations across aging services. It's no longer a question of whether AI will be used, but how to use it responsibly. Used well, it can reduce administrative burden, support staff, and improve access to information. Used without clear direction, it introduces risk - especially around privacy, accuracy, and decision-making.

This toolkit provides a starting point. It helps organizations build a baseline understanding of AI and develop internal policies that set expectations for staff. In a highly regulated, people-centered field, that clarity is essential to protecting residents, supporting staff, and maintaining operational integrity.

This document is intended as an informational primer to help health care organizations understand potential considerations related to the use of artificial intelligence tools and platforms. It is not intended to provide legal advice or to serve as a comprehensive statement of the law or regulatory requirements. Organizations should consult with qualified legal counsel, compliance professionals, information security specialists, and other appropriate advisors when evaluating artificial intelligence tools, conducting HIPAA risk analyses, or implementing policies and safeguards related to the use of these technologies. Each organization's circumstances, systems, and risk profile are unique, and compliance strategies should be tailored accordingly.

SPECIAL NOTE OF APPRECIATION

TO THE TECHNICAL AND LEGAL EXPERTS WHO GENEROUSLY PROVIDED THEIR KNOWLEDGE, GUIDANCE, AND EXPERTISE TO THIS TOOLKIT:

Glen Tibbitts, United Church Homes
Dan Miller, United Church Homes
Michael Gray, Eliza Jennings
Jennifer Griveas, Eliza Jennings
Ben Mounts, National Church Residences
Corey Goldsand, Wexner Heritage Village
Laurinda Johnson, LeadingAge Ohio

Created March 2026

What Is Artificial Intelligence?

Artificial Intelligence, often referred to as AI, describes computer systems that perform tasks that typically require human intelligence.
These tasks may include:

- Summarizing information
- Recognizing patterns in data
- Generating written content
- Identifying trends
- Detecting unusual activity
- Automating repetitive processes

AI does not think or reason independently. It analyzes data and produces results based on patterns it has learned from large amounts of information.

In senior care organizations, AI may already be present in tools used for:

- Electronic health record systems
- Cybersecurity monitoring
- Data analytics and reporting
- Documentation support
- Workforce scheduling

AI should be understood as a support tool. Professional judgment, oversight, and accountability remain essential.

Why Understanding AI is Important

As AI becomes more integrated into healthcare operations, leaders should understand:

- What AI can realistically do
- Where human oversight is required
- How privacy and compliance requirements apply
- The potential risks of misuse or overreliance

A clear understanding of AI supports responsible decision-making and appropriate governance. Artificial intelligence includes a range of related concepts and terminology. The following section defines commonly used terms in clear, practical language.

Key Terms and Definitions

Artificial Intelligence (AI)
Technology that enables computer systems to perform tasks that typically require human intelligence, such as analyzing information, recognizing patterns, generating content, or automating routine processes.

AI Acceptable Use Policy
Organizational guidelines that define how employees may use artificial intelligence tools safely and responsibly.

AI Assistant (Chat-Based AI)
A software tool that interacts with users through conversation to answer questions, generate content, or assist with tasks using artificial intelligence.

Key Terms and Definitions continued...

AI Risk Management
The process of identifying, evaluating, and mitigating operational, privacy, security, and ethical risks associated with artificial intelligence systems.

Algorithm
A defined set of rules or calculations that a computer system follows to complete a task or produce a result.

Approved AI Tool
An artificial intelligence application that has been reviewed and authorized for organizational use based on security, privacy, and compliance requirements.

Audit Trail
A record of system activity that shows who accessed information, what actions were taken, and when. This is important for compliance and monitoring system use.

Automation
The use of technology to perform repetitive tasks with minimal human intervention.

Automation with AI
Technology that combines automation with artificial intelligence to perform routine tasks while adapting based on data patterns.

Key Terms and Definitions continued...

Bias
A systematic error in data or decision-making that can result in unfair or inaccurate outcomes. AI systems may reflect biases present in the data used to train them.

Business Associate Agreement (BAA)
A contractual agreement required when a vendor handles protected health information on behalf of a healthcare organization, as required under HIPAA.

Clinical Decision Support (CDS)
Technology that provides healthcare staff with data-driven insights or recommendations to assist in clinical decision-making. Some systems may use AI to identify risks or patterns in resident data.

Data Governance
Organizational policies and procedures that guide how data is collected, stored, used, and protected.

Data Leakage
Sensitive or confidential information being exposed through AI use.

Data Privacy
The protection of sensitive information from unauthorized access or disclosure. In healthcare, this includes compliance with HIPAA and other applicable regulations.

Key Terms and Definitions continued...

Data Security
The protection of digital information from unauthorized access, corruption, or theft.

De-Identified Data
Health information that has had personal identifiers removed so that individuals cannot be readily identified. This type of data may be used for analytics or system improvement.

Deepfake
AI-created images, video, or audio that convincingly imitate real people.

Electronic Health Record (EHR)
A digital version of a resident's medical and care information. Many AI tools rely on or integrate with EHR data.

Embedded AI
Artificial intelligence features integrated into existing software systems, such as electronic health records, cybersecurity platforms, or scheduling tools.

Enterprise AI
Artificial intelligence tools deployed within an organization's secure technology environment and subject to internal governance, security, and compliance controls.

Key Terms and Definitions continued...

Ethical Risk
AI outcomes conflict with company values, policies, or public expectations.

Explainability
The ability to understand and describe how an AI system reached a particular output or recommendation.

Fine-Tuning
The process of adjusting an existing AI system using additional targeted data to improve performance for a specific purpose.

Generative AI
AI systems that create new content, such as text, summaries, images, or reports, based on patterns learned during training.

Governance
The policies, procedures, and oversight structures that guide how technology, including AI, is used within an organization.

Guardrails
Technical controls or organizational policies are designed to limit how AI systems are used and reduce risk.

Hallucination
An instance in which an AI system generates incorrect or fabricated information that appears credible. AI output should always be reviewed for accuracy.

Key Terms and Definitions continued...

Human-in-the-Loop
A system design in which humans review, approve, or guide AI outputs before decisions are made or actions are taken.

Human Oversight
The requirement that qualified professionals review and take responsibility for decisions or outputs generated by AI systems.

Large Language Model
A type of AI system trained on large volumes of text that can understand and generate human language. Many chat-based tools are powered by these systems.

Machine Learning
A type of artificial intelligence that improves performance by learning from data rather than relying solely on pre-programmed instructions.

Misinformation
AI generating or repeating information that is inaccurate or misleading.

Model
The trained AI system that produces outputs after being developed using data.

Natural Language Processing
Technology that enables computers to understand, interpret, and work with human language in written or spoken form.

Key Terms and Definitions continued...

Predictive Analytics
The use of historical data and statistical methods to forecast potential future outcomes, such as rehospitalization risk or staffing trends.

Privacy Invasion
AI using or revealing personal data in ways people did not expect or approve.

Prompt
The question, instruction, or input provided to an AI system to generate a response.

Prompt Injection
A technique in which a user intentionally or unintentionally provides instructions that cause an AI system to ignore safety guidelines or reveal sensitive information.

Protected Health Information (PHI)
Individually identifiable health information that is protected under HIPAA regulations.

Responsible AI
The practice of using artificial intelligence in a manner that is ethical, secure, transparent, and aligned with organizational values and regulatory requirements.

Key Terms and Definitions continued...

Risk Assessment
A structured evaluation of potential security, privacy, operational, or compliance risks associated with a technology or system.

Secure AI Environment
A controlled technology environment where AI systems operate within defined security protections, data policies, and monitoring processes.

Shadow AI
The use of artificial intelligence tools by employees without organizational approval or oversight.

Training Data
The information used to teach an AI system patterns and relationships. The quality and source of training data influence system performance.

Unapproved AI Tool
An artificial intelligence system that has not undergone organizational review and may not be used for sensitive or protected information.

Vendor Due Diligence
The process of evaluating a technology provider’s security practices, privacy protections, compliance posture, and contractual safeguards before adoption.

AI Risk Tolerance

A risk assessment is a structured evaluation of potential security, privacy, operational, or compliance risks associated with a technology or system. Assessing risk tolerance turns AI decisions into a deliberate strategy instead of a series of ad hoc choices. It allows people to move forward with intention and use new tools in ways that are responsible and sustainable.

AI Risk Tolerance Profiles

Profile 1 — Guarded Adoption

The organization adopts AI in a cautious, tightly controlled manner, prioritizing predictability and risk containment. AI is used primarily to assist human work, not to make or automate consequential decisions. Controls are established before deployment, and human judgment remains central.

Profile 2 — Governed Innovation

The organization adopts AI as a strategic capability, balancing innovation with structured oversight. AI may inform decisions and recommendations, but accountability remains with human decision-makers. Governance frameworks, monitoring, and escalation mechanisms are integral to deployment and scaling.

Profile 3 — Accelerated Experimentation

The organization adopts AI with a higher tolerance for uncertainty in pursuit of speed, efficiency, or competitive advantage. AI may be embedded in core workflows and automation, with an emphasis on rapid iteration. Risk is managed through active monitoring, accountability, and the ability to remediate or suspend AI systems quickly.

AI Risk Appetite Summary

Dimension	Guarded Adoption	Governed Innovation	Accelerated Experimentation
Overall Risk Tolerance	Low	Medium	High
Primary Use of AI	Assistive, internal productivity	Decision support and prioritization	Automation and agentic workflows
Decision Authority	Human-only	Human-led, AI-informed	AI-assisted or AI-executed
Human-in-the-Loop	Always required	Required for high-impact uses	Selective or post-hoc
Governance Approach	Front-loaded approvals and controls	Tiered intake, ongoing oversight	Lightweight gating, continuous monitoring
Data Sensitivity	Low to moderate	Moderate to regulated	Broad, including sensitive data
Tolerance for Error	Very low	Moderate	Higher
Regulatory / Reputational Exposure	Minimized	Managed	Accepted as tradeoff

AI & HIPAA Compliance

Artificial intelligence (AI) tools are rapidly finding their way into healthcare operations. Long-term care organizations in particular are beginning to review and deploy AI systems and tools that assist with documentation, administrative workflow, quality monitoring, and other operational tasks.

There are clear benefits to these technologies. AI can help staff organize information, summarize documents, support policy drafting, and streamline certain administrative functions. Used thoughtfully, these tools can reduce routine workload and help organizations manage large amounts of information more efficiently.

At the same time, their use raises important compliance questions under the Health Insurance Portability and Accountability Act. Most healthcare professionals understand the need to safeguard protected health information (PHI) when working in the electronic medical record, communicating with families, or handling documents.

However, many staff members do not instinctively apply those same privacy considerations when interacting with AI tools. A staff member might recognize that resident information should not be emailed outside the organization but may not think twice about entering the same information into an online AI system. Because of this disconnect, organizations should approach the use of artificial intelligence carefully and evaluate these tools within the existing HIPAA framework. Any technology that may create, receive, maintain, or transmit protected health information should be evaluated through the same compliance and governance processes used for other healthcare technologies.

This primer reviews several key issues organizations should consider when evaluating AI platforms and tools. It addresses the HIPAA Security Rule risk analysis requirement, administrative, technical, and physical safeguards, HIPAA policy considerations, the importance of technology inventories, workforce use of artificial intelligence, minimum necessary considerations, business associate implications, incident response risks, and practical questions compliance leaders should ask before approving new tools.

The Security Rule Risk Analysis Requirement as the Baseline

Before focusing specifically on artificial intelligence, it is important to begin with one of the foundations of the HIPAA Security Rule, which is the requirement to conduct an accurate and thorough risk analysis. The Security Rule requires covered entities to identify potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI). The analysis should examine how information is created, received, maintained, and transmitted across the organization and determine what safeguards are necessary to protect it.

The Office for Civil Rights, which enforces HIPAA, frequently identifies failure to conduct an adequate Security Rule risk analysis as one of the most common compliance deficiencies in healthcare enforcement actions. A risk analysis is not a one-time project, nor is it limited to traditional information technology systems. It must be an ongoing process that reflects how technology, workflows, and interventions evolve over time.

Artificial intelligence technologies present a similar issue. If staff are using AI tools that interact with organizational data and those tools have not been evaluated through the risk analysis process, the organization may expose itself to unnecessary compliance risk.

Conducting the HIPAA Security Rule Risk Analysis

Some organizations assume that a HIPAA risk analysis must be performed by an outside consultant. While many healthcare organizations do engage external experts to assist with the process, HIPAA does not require the use of a consultant.

Risk analyses may be conducted internally using structured frameworks and available guidance, or with the assistance of outside professionals. The U.S. Department of Health and Human Services provides several resources to support organizations conducting risk analyses, including the Security Risk Assessment Tool developed with the Office of the National Coordinator for Health Information Technology.

Regardless of the method used, the risk analysis must be accurate, thorough, and specific to the organization. Importantly, however, any standardized risk tool must be adapted to meet the specifics of the individual organization. A generic template or checklist is not sufficient. The assessment must reflect the systems, workflows, and technologies actually used within the organization.

As organizations begin adopting artificial intelligence tools, those technologies should be evaluated through the same risk analysis process used for any system that interacts with electronic protected health information.

Administrative, Technical, and Physical Safeguards

The HIPAA Security Rule requires covered entities to implement administrative, technical, and physical safeguards to protect electronic protected health information.

Administrative safeguards relate to policies, procedures, workforce training, and organizational oversight. In the context of artificial intelligence, administrative safeguards include developing policies that define when AI tools may be used, training staff on appropriate use, and ensuring leadership oversight when new technologies are introduced.

Technical safeguards involve the technological protections applied to systems that store or process electronic protected health information. When evaluating AI platforms, organizations should consider whether the system stores information, how data is transmitted, whether inputs are retained, and what controls exist for authentication, encryption, and logging.

Physical safeguards address the devices and environments through which information is accessed. Even when an artificial intelligence tool is cloud based, staff may access it through laptops, workstations, or mobile devices. Organizations should ensure that these devices are appropriately secured.

HIPAA Policies and AI

Currently, HIPAA regulations do not specifically reference artificial intelligence. The rules were written before modern AI tools became widely available. However, HIPAA was designed to be technology neutral. The rules focus on how PHI is used, disclosed, and protected rather than on the specific technology involved.

Because of this structure, the HIPAA Privacy Rule, Security Rule, and Breach Notification Rule apply whenever a system creates, receives, maintains, or transmits protected health information, regardless of whether the technology uses artificial intelligence.

Organizations should evaluate whether their policies adequately address the use of artificial intelligence tools and may consider addressing topics such as the appropriate use of AI systems, approved platforms, documentation expectations, training requirements, and vendor review procedures.

The Importance of Inventorying Technology and AI Tools

An effective HIPAA risk analysis depends on a clear understanding of the technologies being used within the organization. Healthcare organizations typically maintain inventories of equipment such as computers, servers, and major software systems that store or transmit resident information. Artificial intelligence tools should be included in the same type of inventory. Without visibility into the technologies being used across the organization, it is difficult to assess risks or determine what safeguards are needed.

Expanding the Technology & AI Inventory

Technology inventories should extend beyond traditional clinical systems. Artificial intelligence capabilities can appear in many forms across an organization, including systems that may not initially appear to process protected health information.

Organizations may consider inventorying the following types of artificial intelligence technologies:

- AI documentation tools used to assist with clinical or administrative writing
- AI transcription or speech recognition systems
- AI-driven clinical support tools
- AI-based quality monitoring or analytics platforms
- AI-powered communication or chatbot systems
- AI tools integrated into electronic medical record systems
- AI tools used by administrative departments for summarization or drafting tasks
- AI browser extensions or plug-ins used by staff
- AI tools embedded within third-party vendor platforms
- AI platforms used to analyze operational, quality, or staffing data

The inventory should also identify how these tools are accessed and how they interact with organizational data. This may include documenting:

- Whether the tool receives protected health information
- Whether data is stored or retained by the vendor
- Whether user inputs are used for system training
- Whether the platform integrates with other systems
- Where the system is hosted or where data is transmitted

Maintaining this level of visibility allows organizations to evaluate risk, implement safeguards, and ensure that new technologies are introduced thoughtfully.

Workforce Use of AI

Many risks associated with artificial intelligence arise from informal workforce use rather than formal enterprise deployment. Staff may use AI tools to draft documentation, summarize reports, or generate written communications. Without clear guidance, employees may assume these uses are acceptable. In practice, entering resident information into an external AI platform discloses PHI to a third party. Organizations should address this risk through training, policies, and oversight.

Minimum Necessary Considerations

The HIPAA Privacy Rule requires that uses and disclosures of PHI be limited to the minimum necessary to accomplish the intended purpose. AI tools can complicate this principle because staff may be tempted to enter entire documents or large amounts of information when requesting summaries or assistance. Organizations should reinforce the importance of limiting the amount of information entered into any system and removing identifiers whenever possible.

Business Association Considerations and Vendor Due Diligence

In some situations, an organization may be evaluating a vendor that offers AI technology directly. For example, the organization may be considering an AI documentation tool, a data analytics platform that incorporates artificial intelligence, or a system that uses AI to summarize reports or analyze operational data.

For this reason, organizations should conduct appropriate vendor due diligence before permitting the use of any AI tool that may interact with PHI or before allowing a Business Associate to use AI when performing services that involve protected health information. Vendor due diligence should include reviewing the vendor's privacy policies, security practices, and contractual terms to understand how the system handles submitted information. Organizations should determine whether data entered into the platform is stored by the vendor, whether it is shared with subcontractors, and whether the vendor provides assurances regarding confidentiality and security. Organizations also are wise to inquire as to whether the vendor's security practices align with the HIPAA Security Rule safeguards.

Findings from the due diligence process may necessitate implementing specific protections or controls related to the vendor's use of AI. These protections may include contractual limitations on how data may be used, requirements for encryption or access controls, limitations on data retention, or additional monitoring and oversight by the organization. Sometimes an organization may determine that a vendor's AI use creates risks that cannot be mitigated. In those situations, the organization may decide not to permit the use of that technology or may restrict how it is used within the organization.

By carefully evaluating both AI vendors and Business Associates that may use AI when handling PHI, organizations can better manage the risks associated with these technologies while maintaining compliance with HIPAA requirements.

AI Incident Response & Breach Risk

AI tools can also introduce incident response and breach notification considerations. For example, a workforce member might paste an incident report, employee investigation documents, or clinical documentation into an AI system to generate a summary. If that platform stores the information or allows vendor access, PHI may have been disclosed outside the organization.

When this occurs, the organization may need to conduct a breach risk assessment under the HIPAA Breach Notification Rule to determine whether the disclosure created probability that the information was compromised.

Practical Compliance Considerations When Evaluating AI

The discussion above highlights how the use of AI intersects with a number of existing HIPAA requirements. While AI continues to evolve, the underlying compliance framework remains the same. When AI tools interact with PHI, organizations should evaluate those technologies within the context of their broader compliance programs.

For many healthcare organizations, the introduction of artificial intelligence raises new questions that should be incorporated into existing governance processes, including but not limited to HIPAA Security Rule risk analyses, vendor oversight procedures, workforce training programs, and incident response planning.

Compliance and information security leaders may find it helpful to step back and consider several practical questions when evaluating artificial intelligence tools:

- Does the system interact with protected health information?
- Has the technology been evaluated through the organization's health care compliance risk analysis and HIPAA Security Rule risk analysis?
- Will a vendor qualify as a Business Associate?
- How does the system handle information entered into the platform, including storage, retention, or potential use for model training?
- Are appropriate administrative, technical, and physical safeguards in place
- Have workforce policies addressed the acceptable use of AI?
- Who is responsible for approving, monitoring, and overseeing the use of these technologies within the organization?

These questions are in no way exhaustive, but they can serve as a useful starting point.

Because the issues surrounding AI often span multiple disciplines, organizations may benefit from involving a team that includes compliance professionals, legal counsel, information security personnel and technology leadership, as well as operational leaders. A collaborative approach can help ensure that emerging technologies are evaluated thoughtfully and that appropriate safeguards are considered before new tools are adopted. By integrating AI considerations into existing compliance structures and governance processes, organizations can better navigate the evolving technology landscape while continuing to safeguard protected health information.

AI tools and platforms offer meaningful opportunities to improve efficiency and support operations. At the same time, their use must be evaluated carefully within the HIPAA regulatory framework. Organizations should ensure that their risk analysis is current, maintain visibility into technologies in use, implement appropriate safeguards, establish clear policies governing AI use, and ensure that staff understand how HIPAA protections apply when interacting with these tools.

This document is intended as an informational primer to help health care organizations understand potential HIPAA considerations related to the use of artificial intelligence tools and platforms. It is not intended to provide legal advice or to serve as a comprehensive statement of the law or regulatory requirements. Organizations should consult with qualified legal counsel, compliance professionals, information security specialists, and other appropriate advisors when evaluating artificial intelligence tools, conducting HIPAA risk analyses, or implementing policies and safeguards related to the use of these technologies. Each organization's circumstances, systems, and risk profile are unique, and compliance strategies should be tailored accordingly.

Sample Policies

The following policies are provided as examples to assist organizations in considering how artificial intelligence (AI) use may be addressed. These samples are not legal advice and are not intended to serve as comprehensive or universally applicable policies. Each organization operates within its own regulatory environment, technology infrastructure, and risk profile. The examples are intended to serve as a starting point for discussion and policy development rather than a substitute for organization-specific analysis. Organizations should consult with legal counsel and other appropriate advisors when developing AI policies.

Sample Policy #1

Overview
[INSERT COMPANY NAME] recognizes that artificial intelligence ("AI") technology will increase employee productivity, innovation, and the quality of the Organization's services and supports the use of AI technology in an appropriate and secure manner consistent with applicable law.
This policy outlines the principles, responsibilities, and acceptable use and governance of AI technology within the Organization, guided by the Organization's overarching AI philosophy:

·We will leverage AI to maintain and enhance our ability to provide high-quality care, services, and communities, using safeguards that honor human dignity and help facilitate the safe, trustworthy, and reliable use of AI.

·Because AI technology is rapidly changing, the Organization recognizes this policy is a starting point in its AI journey. The Organization will continue to explore what the "right" AI tools are, including through formal and informal testing of new AI tools that may advance the mission.

Scope
This policy applies to all AI technology, including large language models ("LLMs"), generative adversarial networks, diffusion models, machine learning, deep learning, neural networks, natural language processing, predictive analytics, anonymous systems, image and video generation, and computer vision. It also supplements and will not be construed to contradict, limit, or replace existing Organization policy.

Appropriate Use of AI

The rules for appropriate use of AI technology are for all [INSERT COMPANY NAME] employees and contractors (1) acting on behalf of or in service to the Organization or an affiliated company or (2) using [INSERT COMPANY NAME] devices, software, access credentials, or other technology platforms.

1. Appropriate Use Generally – "The AI Five". AI technology must be used for legitimate business activities, such as aiding users with job-related tasks for improved productivity, efficiency, and decision-making. Examples where AI technology can be useful include preparing or generating first drafts of correspondence, memoranda, educational materials, and marketing collateral, or sorting, ranking, summarizing, and analyzing large quantities of data, documents, and information, but in each instance must be used consistent with the Confidentiality, Privacy, and Data Protection rules below.

The Organization has designated [DESIGNATED LLM, e.g. CoPilot, ChatGPT] as the LLM/primary AI technology designated for use by Organizational users. Users must use their Organizational email and credentials when using [DESIGNATED LLM, e.g. CoPilot, ChatGPT], rather than any person email or credential.

Employees remain free to try other AI technology, as appropriate, to determine whether that AI technology might be useful to the Organization, so long the use of such AI technology is (1) generic (e.g., to answer generic questions, create generic content, or analyze publicly available information), (2) not involving private Organization, resident, or patient information, and (3) consistent with this policy.

To solidify the rules for appropriate use of AI technology, Organization users must abide by the “AI Five”:

(1) I will use [DESIGNATED LLM, e.g. CoPilot, ChatGPT] , the general AI technology designated for primary use, to enhance my and my team's ability to serve our mission.
(2) I will only use new and not yet approved AI tools generically, that is, without inputting private Organization, resident, or patient information.
(3) I will review AI output to ensure it is safe, trustworthy, and reliable.
(4) I will report any concern with AI use or output, as soon as it arises.
(5) I will use AI consistent with policy, safeguarding information of the Organization and those connected to our mission as if it were my own.

2. Human Review of AI Output. AI technology may produce false, inaccurate, or misleading information, so human review AI output is—and should be—critical, particularly when output is being used, in whole or in part, to make decisions regarding Organization business. This means, for example, that AI technology should not be used to create final content and should not be used as a substitute for independent human judgment.

3. Use of AI Technology in Meetings.

a.Recordings By [INSERT COMPANY NAME] Users - Users may only use [DESIGNATED LLM and/or transcription service, e.g. CoPilot, ChatGPT, Notetaker] for purposes of recording and/or transcribing the substance of meetings using AI technology, and only under the following conditions, with an appropriate license to do so:

i. Meeting attendees receive notice of the AI technology's use;

ii. The meeting is not (i) a parent board or board committee meeting (i.e., use is approved for staff boards: Investment Corp., Affordable Housing, Healthcare, and Corporate Compliance), (ii) a privileged legal meeting, or (iii) a business-to-business meeting that concerns a potential merger, acquisition, or other similarly sensitive or confidential business subject; and

iii. At least one attendee is designated to review—and revise as needed—the tool's output for what occurred during the meeting.

Recordings and draft transcription of all meetings must be deleted within 30 days of the meeting, as they should only be created for informal, short-term purposes and are not an official record of the meeting.

b.Recordings By Third Parties - Users may consent to a third-party recording or transcribing the substance of a meeting via an AI technology under the following conditions:

i. Meeting attendees receive notice of the AI technology's use;
ii. The meeting is one that could be recorded by [INSERT COMPANY NAME];

iii. Users believe the meeting is one that should be recorded;

iv. Users will receive a copy of the recording/transcription;

v. A [INSERT COMPANY NAME] user is designated to review—and revise as needed—the tool's output for what occurred during the meeting, if the notes will be relied on for what occurred during the meeting.

4. Confidentiality, Privacy, and Data Protection.

a. AI technology can collect, store, and use input information, resulting in the disclosure of information to one or more third parties.

b. Consistent with Organization policy and applicable law governing confidentiality, privacy, and protection of sensitive data, users must exercise care in utilizing AI technology to ensure that confidential, proprietary, and sensitive information is not used or disclosed.

c. For Copilot – General/Web AI Use: You may generally insert company information into [DESIGNATED LLM, e.g. CoPilot, ChatGPT] because interactions within Copilot are secure under our enterprise agreement with Microsoft; but, you should not insert the following into [DESIGNATED LLM, e.g. CoPilot, ChatGPT]:

i. sensitive information of an employee, resident, or patient, such as birth dates, social security numbers, contact information, or health information; or
ii. privileged attorney-client communication or attorney work product.

d. For Non-[DESIGNATED LLM, e.g. CoPilot, ChatGPT] Tools – General/Web AI Use: Do not input any confidential, personally identifiable, or sensitive information into an AI technology. Information that should not be deposited into or shared with AI technologies includes the following:

i. personal identifiers, protected health information, and other sensitive personal information such as names, birth dates, social security numbers, account numbers, personal contact information;

ii. sensitive, non-public, confidential, or trade secret information and documents regarding the business of the Organization that would cause harm to Organization or waive privileges if publicly disclosed, including financial information, bank information, attorney-client, attorney work product, or other protected confidential communications, peer-review and quality assurance information, employee names or rosters, sensitive strategic planning materials, or vendors or business partners, including those with whom the Organization has entered into non-disclosure agreements.

5. Reporting AI Concerns & Policy Violations.

a. Users must contact their supervisor or Organizational contact, who will promptly report the concern as a security incident immediately if they become aware of:

i. An actual or possible violation of this policy; or
ii. An approved AI technology generating output that is: (1) clearly erroneous, (2) appreciably inaccurate or misleading, (3) offensive, harassing, or discriminatory, or (4) believed to violate Organization policy.

b. Reports will be reviewed in due course, and users must cooperate with the review and any corrective actions by the Organization.

c. The Organization may, in its sole discretion, suspend use of any AI technology during any such investigation.

AI Governance
The Organization recognizes that governance of AI technology is a team sport that requires a multi-disciplinary team to help build processes to evaluate, select, and monitor the use of AI technology. This team will meet at least twice a year and work on the following:

1) Develop a process for review & approval of new AI technology in the ordinary course of business;

(2) Develop basic metrics for the periodic review of AI technology to ensure it remains safe, trustworthy, and reliable.

(3) Provide recommendations for AI training and upskilling for Organizational employees.

Miscellaneous

1. Amendment. AI technology and the laws and regulations governing AI are rapidly evolving; so, this policy or related policies may be amended from time to time.

Sample FAQs to Supplement Policy

Sample mentioned Copilot as designated platform.

1. What is the purpose of the AI Use & Governance Policy?

The policy is designed to ensure that artificial intelligence (AI) is used to increase productivity, innovation, and service quality in a secure and responsible manner, consistent with applicable laws and organizational values.

2. Who does the AI policy apply to?

It applies to all [INSERT ORGANIZATION] employees and contractors acting on behalf of the organization or using organizational devices, software, or credentials.

3. What are the main rules for appropriate use of AI technology ("The AI Five")?

(1) I will use Copilot, the general AI technology designated for primary use, to enhance my and my team's ability to serve our mission.

(2) I will only use new and not yet approved AI tools, generically, that is, without inputting private Organization, resident, patient information.

(3) I will review AI output to ensure it is safe, trustworthy, and reliable.

(4) I will report any concern with AI use or output, as soon as it arises.

(5) I will use AI consistent with policy, safeguarding information of the Organization and those connected to our mission as if it were my own.

4. What types of information should not be entered into AI tools at this time?

When using Copilot, you may generally insert company information but you should not insert sensitive information of an employee, resident, or patient, such as birth dates, social security numbers, contact information, or health information, or privileged attorney-client communication or attorney work product.

When using new and not yet approved AI tools generically per policy, you should not input any confidential or personal Confidential, personally identifiable, or sensitive information—such as names, birth dates, social security numbers, or protected health information—should not be input into any AI technology.

5. Why is human review of AI output required?

AI can produce false or misleading information. Human review ensures outputs are safe, trustworthy, and reliable, and that professional judgment is always applied before making decisions.

6. What should employees do if they have concerns or notice policy violations related to AI?

Report any concerns or violations to your supervisor or organizational contact (if you are a contractor), who will escalate the issue as a security incident via Aclaimant. Cooperation with investigations and corrective actions is required.

7. What is Microsoft Copilot?

Microsoft Copilot is an advanced AI tool integrated into Microsoft's suite of productivity applications. It assists users with tasks such as drafting documents, analyzing data, and summarizing information, all within familiar Microsoft 365 environments.

8. Why did [INSERT ORGANIZATION] choose Copilot as its primary AI tool?

Copilot was selected because it is provided by Microsoft—a well-known, trustworthy provider—and integrates seamlessly with our existing IT tools and systems, ensuring security and compliance.

9. How does Copilot enhance employee productivity and support our mission?

Copilot helps employees by automating routine tasks, generating first drafts of correspondence, summarizing large volumes of non-sensitive data, and supporting decision-making.

10. How can employees access Copilot?

Employees must use their organizational email and credentials to access Microsoft Copilot. Personal emails or credentials should not be used for organizational work.

11. Can employees use other AI tools besides Copilot?

Employees may try other AI technologies for generic purposes (e.g., answering general questions or analyzing public information), but must not use private or sensitive organizational data with unapproved tools.

12. Can employees use Copilot to record or transcribe meetings?

Yes, with proper licensing, and so long as it's not a meeting where such use is prohibited (see Question 13) and it's done per policy (see Question 14).

13. Are there meetings where employees cannot use Copilot transcription?

Yes, Copilot cannot be used for parent board or parent board committee meetings, privileged legal meetings, privileged legal meetings, or business to business meetings that concern a potential merger, acquisition, or other similarly sensitive or confidential business subject.

14. How do I use Copilot transcription for permitted meetings in line with the AI Use & Governance Policy?

To use Copilot's transcription feature during a Microsoft Teams meeting, follow these steps:

(1) Begin your meeting as usual in Microsoft Teams.
(2) Enable Transcription: o Click the "More" (three dots) option in the meeting control bar. o Select "Record and transcribe," then choose "Start transcription."
(3) Notify and Obtain Consent: Ensure all meeting attendees are notified and have consented to the use of AI transcription, as required by policy.
(4) Review and Revise Output: Designate at least one attendee to review and revise the transcript or notes generated by Copilot to ensure accuracy and completeness.
(5) Delete Recordings Promptly: Recordings and transcripts will be deleted within 30 days of the meeting and will be auto deleted in Teams accordingly, as they are only for informal, short-term purposes and are not official records.

12. Can employees use Copilot to record or transcribe meetings?

Yes, with proper licensing, and so long as it's not a meeting where such use is prohibited (see Question 13) and it's done per policy (see Question 14).

13. Are there meetings where employees cannot use Copilot transcription?

Yes, Copilot cannot be used for parent board or parent board committee meetings, privileged legal meetings, privileged legal meetings, or business to business meetings that concern a potential merger, acquisition, or other similarly sensitive or confidential business subject.

14. How do I use Copilot transcription for permitted meetings in line with the AI Use & Governance Policy?

To use Copilot's transcription feature during a Microsoft Teams meeting, follow these steps:

(1) Begin your meeting as usual in Microsoft Teams.
(2) Enable Transcription: o Click the "More" (three dots) option in the meeting control bar. o Select "Record and transcribe," then choose "Start transcription."
(3) Notify and Obtain Consent: Ensure all meeting attendees are notified and have consented to the use of AI transcription, as required by policy.
(4) Review and Revise Output: Designate at least one attendee to review and revise the transcript or notes generated by Copilot to ensure accuracy and completeness.
(5) Delete Recordings Promptly: Recordings and transcripts will be deleted within 30 days of the meeting and will be auto deleted in Teams accordingly, as they are only for informal, short-term purposes and are not official records.

15. Is it OK if I participate on a call with a third party who records or transcribes the meeting using an AI tool?

Yes, but use your judgment and observe these best practices:

(1) All meeting attendees should receive notice of the AI technology's use;
(2) It's a meeting that a [INSERT ORGANIZATION] employee could record (see Question 13);
(3) You believe it's a meeting that should be recorded or transcribed;
(4) You will receive a copy of the recording/transcription;
(5) You or someone from [INSERT ORGANIZATION] will review—and revise as needed—the tool's output for what occurred during the meeting, if the notes will be relied on for what occurred during the meeting.

16. Where can employees find free resources or training on using Copilot?

Employees have several options for accessing free, official Microsoft Copilot training:
• Microsoft Learn: Microsoft's official learning platform offers a dedicated Get Started with Microsoft 365 Copilot learning path. This includes beginner-friendly modules, practical demos, and best practices for using Copilot. No prior AI experience is required. [learn.microsoft.com]
• Microsoft Copilot Academy (via Viva Learning): If you have a Microsoft 365 Copilot license, you can access the Copilot Academy directly through Viva Learning. The Academy provides structured, hands-on courses and is available in multiple languages. No additional registration is needed. [learn.microsoft.com]
• Microsoft 365 Copilot Video Tutorials: Microsoft Support offers a library of video tutorials covering Copilot basics, prompting tips, and practical use cases for everyday work.

• Live and On-Demand Events: Microsoft regularly hosts free Copilot training events and webinars, featuring expert-led demos and Q&A sessions. These events are open to all users and cover real-world scenarios and role-based topics. [microsoft.com]

Sample Policy #2

Overview and Purpose
This policy explains how Artificial Intelligence (AI) can and cannot be used within the organization. It ensures we protect residents, follow all privacy laws, and use technology responsibly. This policy applies to all employees, contractors, and vendors. It covers any AI tool used for clinical work, administrative work, operational tasks, or communication.

Policy

1. Definitions

Artificial Intelligence (AI): Computer tools or systems that can think or perform tasks that normally require a human, such as summarizing information, generating text, recognizing patterns, or answering questions.
High-Risk AI: Tools that influence medical decisions, resident safety, or regulatory documentation.
Limited-Risk AI: Tools used for basic administrative help, such as drafting templates or scheduling tasks.
Sanctioned AI Tool: Any AI tool that has been reviewed and approved by IT, Compliance, and Leadership.

2. Policy Statements

2.1. Human Oversight Is Required
AI may help with tasks, but it cannot make decisions on its own. All clinical, operational, and administrative decisions must be reviewed and confirmed by qualified staff. AI does not replace human judgment or ethical responsibility.

2.2. Approval Is Required Before Using Any AI for Work
Any AI tool used for work must be approved by IT before staff use it. This includes tools used for writing, scheduling, summarizing, image generation, or communication. Employees may not sign up for or use outside AI tools for work without approval.

2.3. No PHI or Confidential Information May Ever Be Uploaded
Employees may never upload, type, paste, or insert any of the following into an AI tool unless it has been formally approved for use by the organization: Protected Health Information (PHI), resident or patient information, internal documents, proprietary business information, employee information, or vendor information. This includes free or publicly available AI systems such as ChatGPT, Google Gemini, Microsoft Copilot, Claude, Grok, DeepSeek, or any similar tool.

2.4. No AI Will Be Added to Company Systems Without Review
The organization will not activate or adopt AI features in company software, communication platforms, electronic records, or equipment until IT reviews system security, Compliance confirms HIPAA and regulatory protections, Leadership approves the tool, vendor agreements include required privacy protections, and a formal data and security assessment is completed.

2.5. Vendor Requirements
Vendors providing AI tools must sign Business Associate Agreements when required, provide information on how their AI works and how bias is monitored, allow human override, provide audit logs, and comply with HIPAA and all privacy laws.

2.6. Use Restrictions and Prohibited Activities

Staff may not upload PHI or confidential information into any unapproved AI tool, use AI to complete clinical documentation, use AI in place of required assessments, enter internal documents or proprietary information into public or free AI tools, or use AI to interpret resident behavior without human review. Violations may violate the Conduct and Behavior Policy, the HIPAA Privacy and Security Policies, and the company Data Protection and Information Security policies. These violations may result in disciplinary action up to and including termination of employment.

2.7. Resident-Centered Use

Any AI used for resident engagement or monitoring must respect privacy, dignity, and individual needs, allow human override, include staff training, and be reviewed regularly for accuracy and appropriateness.

2.8. Ongoing Monitoring

Approved AI tools will be reviewed regularly for accuracy, assessed for fairness and bias, and removed or updated if they become unsafe or unreliable.

2.9. Transparency When AI Is Used in Resident-Facing Materials

If AI is used to create or support any material that will be given to or viewed by residents, families, or their representatives, the organization must be fully transparent. Staff must include a simple notice such as, “This information was developed with the help of an AI tool and reviewed by staff for accuracy,” so residents and families understand that AI assisted in the content and that a staff member confirmed it is appropriate before sharing.

Procedure

1. AI Tool Review Process
IT and Compliance will maintain an inventory of all approved AI tools, including vendor information, risk level, data use, and whether PHI is involved. No AI tool may be used until it appears on the approved list.

2. AI Risk Assessment
Before approval, every tool must undergo a review that examines whether PHI will be used, how data is stored and secured, human override capabilities, potential for bias, and compliance with HIPAA and state regulations.

3. Staff Training
Staff will receive training on what AI is and how it works, how to use AI responsibly, what information cannot be entered into AI tools, how to disclose AI use to residents and families when required, and how to report concerns about AI use or behavior.

4. Enforcement
Violations of this policy may violate the Conduct and Behavior Policy, the HIPAA Privacy and Security Policies, or the company Data Protection and Information Security policies. Violations may result in disciplinary action up to and including termination. All staff must immediately report any concerns about AI misuse or unusual AI behavior.