Acceptable Uses and Governance of Artificial Intelligence Policy

REFERENCES/RELATED:

PATIENT PRIVACY AND CONFIDENTIALITY #220.00, SOFTWARE MANAGEMENT AND USAGE #405.00, COMPUTER USAGE POLICY #400.00, TEMPLE UNIVERSITY HEALTH SYSTEM INFORMATION SECURITY AND PRIVACY COMPLIANCE PROGRAM, PRIVACY AND NON-DISCRIMINATION NOTICES

ATTACHMENTS:

None.

I. SCOPE

This policy shall apply to Temple University Health System, Inc. (TUHS) and all TUHS subsidiary corporations. Any reference to TUHS in this policy shall include TUHS and its 501(c)(3) tax-exempt subsidiaries.

II. DEFINITIONS

For purposes of this policy, the following terms shall have the meanings set forth below:

Artificial Intelligence ("AI") refers to machines that mimic human intelligence and human cognitive functions like problem-solving and learning. AI is a broad term that includes many different techniques and applications, including, but not limited to, the following:

- **Machine Learning:** a form of AI based on algorithms trained on data. These algorithms can detect patterns and learn how to make predictions and recommendations by processing data and experiences. The algorithms also adapt in response to new data and experiences to improve their efficacy over time.

- **Deep Learning:** a type of machine learning that can process a broader range of data resources (images, for instance, in addition to text), requires even less human intervention, and can often produce more accurate results than traditional machine learning. Deep learning uses neural networks—based on how neurons interact in the human brain—to ingest data and process it through multiple iterations that learn increasingly complex data features.

- **Generative AI:** deep-learning models that can take raw data and "learn" to generate new, original content when prompted, rather than simply recognizing or analyzing existing data. These models aim to create new content, such as text, images, video, and audio, that is indistinguishable from what humans might create.

Confidential Information refers to any information that is marked or otherwise identified as confidential by or on behalf of TUHS, information as to which TUHS has confidentiality obligations under law, regulation, or contract, and any other information that would appear to a reasonable person to be confidential under the circumstances. Confidential Information includes the following:

- **Proprietary Information:** information or data learned or created by TUHS (or its employees) which is not generally known to the public and which has some commercial or competitive value to TUHS. Examples of proprietary information include non-public financial records, transaction data, intellectual property, trade secrets, pricing information, business strategies, compensation levels, marketing information, supplier/vendor information, and technology developed in-house.

- **Protected Health Information (PHI)**: any information, whether oral or recorded in any form or medium, that relates to the past, present, or future physical or mental health or condition of any individual or the past, present, or future payment for the provision of health care to an individual.

- **Designated Record Set**: a patient's record of any medical treatment she/he received containing PHI. Such records may consist of inpatient/outpatient medical records, billing records for the provision of medical services, information relating to an individual's enrollment for a health insurance program, healthcare payment information, or medical claims adjudication information.

- **Personally Identifiable Information**: information that can identify an individual when used alone or with other relevant data.

- **Sensitive Information**: sensitive patient information related to drug and alcohol use, mental health, HIV/AIDS, and genetic testing that is subject to special disclosure rules under federal and state laws.

De-identified PHI excludes all the direct identifiers of an individual or the relatives or household members of the individual.

III. PURPOSE

TUHS recognizes that AI tools can increase employee productivity, improve clinical care, and foster innovation. TUHS supports using AI in a safe, ethical, and secure manner. At the same time, TUHS recognizes that AI can pose risks to our operations and patients. AI tools have potential drawbacks, such as bias and hallucination (i.e., nonsensical or inaccurate results), which require human oversight, particularly in healthcare. This policy aims to provide a set of standards by which AI tools are evaluated, implemented, and used across TUHS. This policy is designed to promote the effective use of AI to support patient care and TUHS operations while upholding ethical standards, complying with regulatory requirements, ensuring data privacy and security, and mitigating risks associated with using AI.

IV. POLICY

A. **Compliance with Existing Policies**

This Policy is intended to add to existing policies and legal requirements, all of which remain in full force and effect. Any use of AI under this Policy must comply with the relevant policies, internal controls, and guidelines of TUHS, including TUHS's Patient Privacy and Confidentiality Policy (#220.00), Software Management and Usage Policy (#405.00), Computer Usage Policy (#400.00), and Information Security and Privacy Compliance Program.

B. **Use of Existing and Available AI Tools**

AI tools should not be used to replace human judgment. All TUHS employees and contractors are expected to use these technologies responsibly and ethically, ensuring the tools are used only for approved purposes. The user of AI bears responsibility for any actions or decisions made based on any AI output.

AI should only be used in accordance with the Guidance Regarding the Use of AI published pursuant to this Policy (see Section V.B below).

Patient safety and welfare must be prioritized when the use of AI can affect patient care.

AI (particularly Generative AI) can create inaccurate (also called "hallucinated") information. All content generated by any AI tool must be reviewed and fact-checked by the TUHS employee or contractor using such a tool. An ongoing process that monitors and audits the outputs or results of an AI method may be implemented to ensure the continuing quality and reliability of the model.

To protect the privacy of our patients and the confidentiality of TUHS's internal information, no Confidential Information may be shared with any AI tool without approval from IT Governance and the TUHS Legal Department. A Business Associate Agreement must be in place before any PHI is shared with any third-party AI tool. PHI can be shared only if in compliance with TUHS's Privacy and Non-Discrimination Notices. **No PHI, De-Identified PHI, or PII will be shared with any AI tool unless IT Governance and the TUHS Legal Department approve it.**

AI tools may not be used for illegal or unethical activities, including disseminating false information, cyberbullying or harassment, intentional discrimination, generating illegal or malicious code, or attempting to gain unauthorized access to systems or networks.

Failure to adhere to this Policy or any applicable laws, regulations or rules will be considered a violation of the TUHS Standards of Conduct that may result in appropriate disciplinary action.

V. PROCEDURE

A. **Approval Process**

Any implementation of AI or any new proposed use of AI in support of the health system must be reviewed and approved by the IT Governance Committee and the TUHS Legal Department. Approval shall specify the allowable uses of the AI tool and any limitations on use. Requests must be approved before any specific vendor is selected. The IT Governance Committee may delegate review and approval to other established committees at its

discretion.

IT Governance will establish and update, as necessary, Guidelines for the Review of AI to ensure that the AI utilized by TUHS complies with regulatory requirements and common AI principles: results are valid and reliable, AI systems are safe, secure and resilient, outputs are accountable and transparent, and data usage is privacy-enhanced, fair, and equitable. The IT Governance Committee may delegate responsibility for maintaining these guidelines to other appropriate committees or personnel.

TUHS IT will maintain a list of approved and available AI tools and their associated acceptable uses. TUHS IT will be responsible for conducting periodic reviews of the list, at least annually, to ensure that each AI tool continues to comply with this Policy and the Guidelines for the Review of AI.

B. **Guidelines and Education**

TUHS IT will maintain and internally communicate written Guidance Regarding the Use of AI to assist TUHS employees with understanding the acceptable and prohibited uses of available AI tools.

TUHS IT and TUHS Compliance will be responsible for providing ongoing training and communication to build awareness on the appropriate use of AI technologies, the risks, and benefits of using AI, and criteria that should be considered to evaluate new uses of AI.