Pennsylvania TRAUMA SYSTEMS Foundation

Policy IT-107

Artificial Intelligence (AI) Acceptable Use

Purpose

This policy establishes responsible and secure use of Artificial Intelligence (AI) technologies at PTSF. It aims to:

A. Protect sensitive and regulated data
B. Minimize legal, ethical, and security risks
C. Enable safe, high-impact AI adoption aligned with PTSF's mission

1. Scope

This policy applies to all employees, contractors, volunteers, and board members, who access PTSF systems or process PTSF data. It covers:

A. General-purpose AI assistants (e.g., ChatGPT, Claude, Gemini)
B. AI features embedded in software products (e.g., Microsoft Copilot, Google Workspace AI features)
C. PTSF-built AI applications and automations
D. AI Meeting and Notetaker Tools (e.g., Microsoft Copilot in Teams, Google Meet AI features)
E. Standalone tools with written consent by Elevated and PTSF President

2. Guiding Principles

All AI activities within PTSF must align with the following principles

A. Sensitive information: Never enter private or stakeholder confidential information into any unapproved AI tools.
B. You are responsible and accountable for the outputs of AI. It is essential to thoroughly review and validate the information before relying on it for any decisions or actions.

3. Data Handling Guidelines

AI usage is permitted only within AI services that have been explicitly approved, in writing, by PTSF ("Approved AI Services") and in line with the following requirements. If a particular use would involve mixed data falling into multiple categories, the strictest set of requirements applies. (e.g., a use that includes both public information and internal non-confidential data would be limited to Approved AI Services with no model training).

Data Type	Allowed	Requirements
Public Information	Yes	Use Approved AI Services only
Internal Non-Confidential Data	Yes	Use Approved AI Services with no model training
Confidential Data (redacted/anonymized)	Yes	All mandatory safeguards (Section 5) must be met
Personal Identifiable Information (PII)/Protected Health Information (PHI) or Raw Confidential Data	No	Requires President and legal counsel approval with documented safeguards

Key Principles: Use minimum necessary data; redact or tokenize sensitive fields; avoid free-text pastes of large datasets; prefer system-to-system integrations with logging where available.

4. Mandatory Safeguards

Before entering any confidential or regulated data into an Approved AI Service, all of the following must be true:

A. No model training will be permitted on PTSF data (vendor setting and contract).
B. Data retention by the Approved AI Service is limited or disabled; administrators can configure or request deletion.
C. Single Sign-On (SSO)/Multi-Factor Authentication (MFA) and access controls are enforced where technically feasible.
D. AI services only access content users already have permission to view.
E. Prompts and outputs are logged where technically feasible to allow for auditing.
F. Sensitive fields are removed, masked, or narrowed to the minimum necessary to accomplish the task.
G. All outputs must undergo accuracy and bias checking prior to use. Outputs used externally or for decisions must undergo fact-accuracy checking and peer review.
H. Third-party plugins and extensions must be disabled by default; only vetted and approved plugins and extensions may be used.
I. Vendor risk (security, privacy, compliance) is reviewed by PTSF and legal counsel, where necessary; data processing agreements (DPAs)are in place.
J. DPAs or Business Associate Agreements (BAAs) are in place with AI vendors processing PII/PHI. All processing of PII or PHI through an Approved AI Service must be approved, in writing, by the President and reviewed and approved by legal counsel.

5. Acceptable vs. Prohibited Uses

A. Acceptable Uses (examples):
    i. Ideation and brainstorming for programs and initiatives
    ii. Editing and tone adjustments for communications
    iii. Drafting internal or external communications with review
    iv. Summaries of documents the user is authorized to access
    v. Generating non-production datasets (synthetic) for testing
    vi. Using approved AI meeting assistants to transcribe and summarize meetings where all participants have provided explicit consent and no PHI or confidential matters are discussed
    vii. Generating meeting action items and follow-up tasks from AI transcripts with human review

B. Prohibited Uses (examples):
   i. Using PHI
   ii. Uploading sensitive data to unapproved tools
   iii. Using AI to bypass security controls
      a. Using AI tools to circumvent access controls or audit logging
   iv. Creating misleading or discriminatory content
   v. Relying on AI without human review for accuracy and bias
   vi. Entering passwords, credentials, encryption keys, or security vulnerabilities
   vii. Recording or transcribing meetings without explicit consent from all participants
   viii. Using AI meeting tools in discussions involving PHI, confidential trauma center data, personnel matters, or any other confidential information
   ix. Relying solely on AI-generated meeting minutes without human review and correction
   x. Sharing AI meeting transcripts outside PTSF systems or to unauthorized individuals

6. Prompt Hygiene & Quality

To get the best results from AI tools while protecting sensitive information, follow the CHAT framework:

Context: Where and in what context will this content be used? Provide relevant background without unnecessary sensitive details. Use redaction or placeholders when possible.

Hone: Specify the boundaries of the output you want. Define the scope, required length or format, what to include or exclude, and whether you need plain language or technical phrasing.

Audience: Who are you targeting? Stating the audience helps tailor the language, depth, and examples to the reader.

Tone: Should the output be formal, casual, or something in between? Are you aiming to inform, persuade, or entertain?

After you get a draft: Verify facts and sources (hallucination check), review for bias, and label AI-assisted content where required by this policy.

7. Embedded AI in Software

Treat AI features inside software applications (such as Microsoft Copilot or Google Workspace AI features) as separate processors. Ensure the vendor has equal or stronger safeguards than this policy. Coordinate with IT/Security before enabling new AI features or connecting data sources.

8. Education Requirement

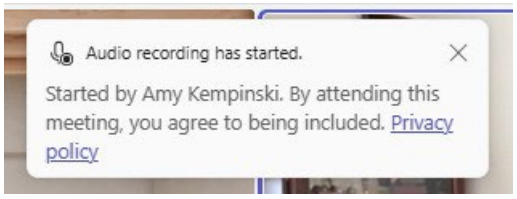
PTSF Employees must complete the Microsoft Teams Breach Secure Now Microsoft Artificial Intelligence Awareness Trainings prior to use.

A. From 2026 this includes:
   i. Artificial Intelligence (AI) Cybersecurity Training (16 minutes)
   ii. Microsoft Copilot Fundamentals (25 minutes)
   iii. ChatGPT Fundamentals (38 minutes)
   iv. Artificial Intelligence for Healthcare (18 minutes)
B. To demonstrate compliance, employees must complete training within 30 days of assignment.
C. Employees will be assigned an AI module as a component of annual training thereafter.

9. AI Meeting Assistants and Note Taking Tools

AI-powered meeting recordings, transcription, and note-taking tools require special consideration due to consent requirements, participant privacy, and the sensitivity of discussions at PTSF.

A. Consent and Notification Requirements:
   i. Obtain explicit consent from ALL meeting participants before activating any AI meeting assistant or recording tool
      - Meeting invite and agenda must indicate “AI assistant and recording tool will be utilized”
   ii. Announce at the beginning of each meeting that an AI tool will be recording/transcribing
      - The meeting organizer will begin recording
      - If using TEAMS; participants will receive a notification



      - If using another format, the organizer must verbally announce the recording tool will be utilized.
   iii. Document consent in the meeting record (e.g., "All participants consented to AI notetaking")
   iv. Respect any participant's choice to decline; if any participant objects, do not use the AI tool for that meeting

B. Prohibited Meeting Types:
   i. Meetings discussing specific patient cases or PHI
   ii. Confidential trauma center performance reviews or accreditation decisions

iii. Executive sessions of the Board of Directors
iv. Disciplinary or personnel matters
v. Attorney-client privileged communications
vi. Any meeting where a participant has declined consent

C. Approved Meeting Types:
   i. General staff meetings and team check-ins
      - Internal PTSF staff meetings do not require explicit consent prior to every meeting. See employee handbook for additional information.
   ii. Project planning and coordination meetings
   iii. Educational sessions and training
   iv. External stakeholder meetings such as partnering organizations
   v. Committee meetings where no confidential personnel or PHI matters are discussed

D. Additional Safeguards:
   i. Pause or disable the AI tool if sensitive topics arise unexpectedly during a meeting
   ii. Review auto-generated meeting minutes before distribution to ensure accuracy and remove any sensitive information that should not have been captured
   iii. Store meeting transcripts and AI-generated notes in PTSF's approved secure storage locations only
   iv. Delete meeting recordings and transcripts when no longer needed per PTSF's record retention schedule
   v. Ensure AI meeting tool vendors meet all requirements in Section 3 (Mandatory Safeguards), including no model training on PTSF data
   vi. Notify external meeting participants (trauma centers, consultants, board members) in advance if AI tools will be used, ideally in the meeting invitation and agenda

E. Host Responsibilities:
   The meeting organizer/host is responsible for:
   i. Determining whether AI notetaking is appropriate for the meeting content
   ii. Obtaining and documenting consent from all participants
   iii. Configuring the AI tool properly (e.g., ensuring recordings stay within PTSF systems)
   iv. Reviewing outputs before sharing
   v. Ensuring compliance with this policy

10. Incident Reporting

Report suspected AI-related incidents (data leakage, insecure outputs, harmful content, or policy violations) per Policy IT-102: Security Incident and Breach Notification and IT-04: Incidence Response Plan.

In the event of an AI service outage or data loss incident, recovery procedures will follow IT-103: Disaster Recovery Plan.

Original Date: 05/21/2026
Review Date:
Revise Date:

Amy Kempinski, MSN, RN, CEN, TCRN — President