HealthWest
Muskegon's Behavioral Wellness Connection

Policy Title: Use of Artificial Intelligence	**Policy #:** 05-028	**Review Dates**	
Category: IT **Subject:** Use of Artificial Intelligence	**Prepared by**: Name: Randi Bennett Title: Director of Information Systems **Approved by:** DocuSigned by: Rich Francisco AA7EBD48ABB04A3... Rich Francisco, Executive Director		
	Effective Date: 03/01/2026	**Last Revised Date:**	

I. PURPOSE

This policy establishes guidelines for the responsible and ethical use of Artificial Intelligence (AI) technologies within HealthWest. It provides guidance for compliance with the Health Insurance Portability and Accountability Act (HIPAA), State of Michigan laws, federal regulations, Muskegon County policies, and internal agency standards.

II. SCOPE

This policy applies to all employees, contractors, interns, volunteers, and third-party vendors who access, implement, or interact with AI tools or systems within the agency's operational environment.

III. DEFINITIONS

- Artificial Intelligence (AI): Any software or system that performs tasks typically requiring human intelligence, including but not limited to natural language processing, machine learning, predictive analytics, and automated decision-making.
- Protected Health Information (PHI): Individually identifiable health information protected under HIPAA.
- Approved AI Tools: AI-enabled systems, applications, or platforms that have been reviewed, vetted, and explicitly approved by one or more of the following authoritative roles within the Information Technology department:

    - Network Security and Systems Manager
    - IT Operations Manager
    - Director of Information Systems
    - Chief Information Officer

IV. POLICY

1. Use of AI Tools
   - Only AI tools and applications that have been explicitly reviewed and approved by one or more of the following authoritative roles within the Information Technology department may be used within the agency: the Network Security and Systems Manager, IT Operations Manager, Director of Information Systems, or Chief Information Officer.
   - Any system or software implemented by HealthWest IT that includes an enabled AI component shall be considered approved for use.
   - Staff must not independently download, install, or use third-party AI tools or browser extensions without prior review and approval by the Network Security and Systems Manager. In the event the Network Security and Systems Manager is unavailable, the Operations Manager, Director of Information Systems, or Chief Information Officer may review and approve such requests to ensure proper oversight and continuity.
   - All content produced with approved AI tools must be reviewed by a qualified team member to verify accuracy, completeness, and alignment with organizational standards before it is used, shared, or implemented.

2. Handling of PHI
   - AI tools must not be used to process, transmit, store, or analyze PHI unless:
     - The tool has been reviewed and approved by one or more of the following authoritative roles within the Information Technology department: the Network Security and Systems Manager, IT Operations Manager, Director of Information Systems, or Chief Information Officer.
     - The tool complies with HIPAA and relevant data protection standards.
     - A Business Associate Agreement (BAA) is in place if required.

   - Staff must avoid entering PHI into public or consumer-grade AI platforms (e.g., ChatGPT, Google Bard, etc.) unless explicitly authorized, configured for HIPAA compliance, and formally approved through the process above.

3. Compliance with Laws and Regulations
   - All AI usage must comply with:
     - HIPAA and related federal privacy and security rules.
     - State of Michigan laws, including the Mental Health Code and data privacy statutes.
     - Muskegon County policies governing technology and data use.
     - Agency-specific policies on confidentiality, data governance, and ethical practice.

4. Transparency and Accountability
   - Staff and clients must be informed when interacting with AI-enabled systems.
   - Clients have a right to decline the use of AI-enabled systems during their clinical session.
   - AI outputs must be reviewed by qualified personnel before being used in clinical decision-making, finalized clinical chart documentation, or client communication.

5. Training and Education
   - All staff are required to complete mandatory training on responsible information technology use. This training covers topics such as artificial intelligence, data privacy, and cybersecurity.
   - Ongoing education will be provided as AI tools evolve and new technologies are introduced.

Prohibited Practices:

- Using unapproved AI tools for any agency-related task.
- Inputting PHI into AI systems that are not configured for HIPAA compliance, lack an associated Business Associate Agreement where applicable, and/or have not been reviewed and approved by one or more of the following authoritative roles within the Information Technology department: the Network Security and Systems Manager, IT Operations Manager, Director of Information Systems, or Chief Information Officer.
- Relying solely on AI-generated content for clinical decisions without human oversight.
- Circumventing IT protocols to enable AI features in unauthorized software.

V. ENFORCEMENT

Any employee, vendor, client, volunteer, intern, or contractor found to have violated this policy may be subject to disciplinary and/or legal action.

Suspected breaches must be reported to:

- IT Department, specifically one of the following roles: Network Security and Systems Manager, IT Operations Manager, Director of Information Systems, or Chief Information Officer
- Compliance Officer
- Privacy Officer

Authors Initials RB/hb