St. Clair County Community Mental Health
Providing Opportunities for Health, Wellness, & Connection

Administrative Policy

Policy Title:	**Artificial and Augmented Intelligence Use**
Policy #:	**08-001-0025**
Effective Date:	09/24/2025
Approved by:	Telly Delor, Chief Operating Officer
Functional Area:	Information Management
Responsible Leader:	Dann Hayes, IT & Security Director
Policy Owner:	Chase Sherman, IT Technician
Applies to:	Community Agency Contractor, Contracted Network Providers, Directly Operated Programs, SCCCMH Staff, SCCCMH Board

Purpose: The purpose of this policy is to establish guidelines for the safe, ethical, and effective use of *artificial intelligence (AI)*, including *augmented intelligence* within St. Clair County Community Mental Health.

I. Policy Statement

It is the policy of St. Clair County Community Mental Health (SCCCMH) to promote the responsible, ethical, and legal use of *AI tools* and technology in support of clinical and administrative functions.

II. Standards

A. General Guidelines

1. Use of AI Tools

- Use of AI tools is solely for tasks that contribute directly to SCCCMH objectives and duties and are in alignment with applicable policies, procedures, and law.
- SCCCMH must not authorize the use of AI systems or technologies that introduce overall risk or health inequities beyond SCCCMH's capabilities to mitigate.
- Employees are only allowed to use AI tools approved by SCCCMH.
- Employees must not share access to SCCCMH AI tools with unauthorized individuals or third parties through the use of login credentials or other means.

2. **AI Tool Approval**
    - Use of AI tools must be evaluated for security, functionality, regulatory compliance, a comparative product review, and risk considerations before use. Evaluation and approval by an interdepartmental collaboration that includes members of Information Technology (IT), Data Management, Corporate Compliance, and any departments with subject matter expertise in areas affected by the AI tool is required.
    - Evaluation requires a risk-based approach where the level of scrutiny, validation, and oversight is proportionate to the overall potential for harmful or biased consequences the AI tool might produce.
3. **Security Review**
    - Each AI tool will be assessed for terms of service, insurance coverage, privacy policies, and third-party involvement.
4. **Clinical Decision Making**
    - Clinical decisions influenced by AI must be made with early and frequent human intervention points during the decision-making process. When AI is used in a manner which impacts access to care or medical decisions at the point of care, the use of AI should be disclosed and documented to served individuals.
5. **Confidentiality**
    - Privacy and confidentiality of information must be prioritized.
    - Employees must not upload or input confidential, proprietary, or *Protected Health Information (PHI)* data into AI tools without prior authorization from the Privacy Officer. This includes data related to served individuals, employees, community members, etc.
6. **Reputable Sources**
    - Only AI tools from reputable vendors with strong security protocols may be used. At a minimum, AI developers must disclose the technology's regulatory approval status applicable consensus standards and clinical guidelines used in design, development, deployment, and continued use of the technology. AI developers/vendors must provide a clear description of problem formulation and intended use accompanied by clear instructions for use.
7. **Training**
    - Employees must complete training on AI functionality, limitations, and ethical considerations before using AI tools.

8. **Exceptions**
    - Any exception to this policy must be approved by the IT Director, in consultation with the Leadership Team prior to any actions taken.
9. **Non-Compliance**
    - Violations of this policy will result in disciplinary action, up to and including termination of employment.

B. Clinical Documentation

1. **Validation**
    - AI-generated clinical notes must be reviewed and approved by clinical staff before inclusion in the *Electronic Health Record (EHR)*.
    - Review should include proofreading, editing as necessary, and engaging in human oversight in the final review process.
2. **HIPAA Compliance**
    - Use of AI in clinical documentation must adhere to HIPAA and other relevant privacy laws. Served individuals must provide informed consent when their information is processed using AI tools.
3. **Bias and Accuracy**
    - AI-generated *output* will be evaluated for bias, fairness, and accuracy as part of SCCCMH's utilization management practices.

C. Prohibited Uses

1. **Employment Decisions**
    - AI tools must not be used for hiring, promotion, or disciplinary decisions.
2. **Personal Information**
    - No personal information (e.g., names, addresses) may be uploaded or entered into AI tools.
3. **Transfer of AI-generated Output**
    - AI output must not be generated using personal or non-SCCCMH work devices and downloaded or otherwise transferred into SCCCMH computers, mobile devices, network resources/equipment, or software, including the electronic mail system or EHR platform.
4. **Original Work Misrepresentation**
    - AI outputs must not be presented as an employee's original work without appropriate disclosures.

5. Exploitation

Two specific uses of AI tools are prohibited as a matter of SCCCMH policy.

- Dark Patterns. AI tools may not be used to distort, trick, or otherwise interfere with the ability of an individual to make independent and informed choices or decisions, or otherwise manipulate a person through subliminal techniques, or so-called dark patterns, to make (or not make) a particular decision or take/refrain from a particular action
- Exploiting Vulnerabilities. AI tools may not be used to exploit potential vulnerabilities of an individual or to distort or impair their ability to make independent and informed choices or decisions or otherwise manipulate or cause physical or psychological harm to themselves or others.

III. Procedures, Definitions, and Other Resources

A. Procedures

Actions

Action Number	Responsible Stakeholder	Details
1.0	IT, Corporate Compliance, and Data Management	1. Conduct security, risk, and compliance reviews for AI tools, including reviewing AI tools and their outputs for biased and discriminatory outputs and applicable legal requirements and SCCCMH policies. 2. Conduct audits, network monitoring, and periodic evaluations. 3. Provide training and technical support for employees 4. Monitor and assess outputs for bias and discrimination across the AI lifecycle.
2.0	SCCCMH Leadership Team	5. Oversee policy implementation and allocate resources for technology, training, and compliance monitoring.
3.0	All SCCCMH Employees	6. Review AI-generated output for accuracy and confidentiality. 7. Immediately report to IT and Corporate Compliance any suspected or actual inadvertent disclosure of confidential, proprietary, or PHI data.
4.0	Clinical staff, and all staff who create, use, or manage data and information	8. Review documentation created with AI-generated output for accuracy and confidentiality by proofreading, editing as needed, and engaging human oversight in the final review process. 9. Ensure compliance with clinical and ethical standards.

B. Related Policies

N/A

C. Definitions

1. *Artificial Intelligence (AI)*: Simulation of human intelligence by machines, that for a given set of human-defined objectives, can make predictions, recommendations or decisions influencing real or virtual environments. AI tools can simulate learning, reasoning, and decision-making.
2. *Augmented Intelligence*: A subset of AI that enhances human capabilities through collaboration with AI systems.
3. *AI Tool(s)*: Any Artificial Intelligence and Machine Learning technologies both individually and collectively, unless otherwise specified within the context of its use.
4. *Electronic Health Record (EHR)*: A digital record of patient health information, maintained securely and accessible by authorized users.
5. *Output*: Any outcome, language, data, or other result, action, or decision obtained from or otherwise performed by or with the assistance of, an AI tool.
6. *Protected Health Information (PHI):* Individually identifiable health information that is transmitted or maintained by electronic media or in any other form or medium. PHI does not include information: i) in education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. § 1232g; ii) in psychotherapy notes; iii) in records described at 20 U.S.C. § 1232g(a)(4)(B)(iv); and iv) in records of individuals who have been deceased for more than 50 years.

D. Forms

N/A

E. Other Resources (i.e., training, secondary contact information, exhibits, etc.)

N/A

F. References

1. HIPAA Privacy Rule (45 CFR Part 164)
2. Michigan Mental Health Code (Act 258 of 1974, Section 330.114)
3. American Recovery and Reinvestment Act of 2009

IV. History

- Initial Approval Date: 08/13/2025 BY: AI Use Working Group, Dann Hayes, Michelle Measel-Morris, Joy Vittone
- Last Revision Date: BY:
- Last Reviewed Date: BY:
- Non-Substantive Revisions: N/A
- Key Words: artificial, augmented, intelligence, bias, discrimination, HIPAA, PHI, confidential, AI, computer, software, internet, bot, tool, output, generate, consent, accurate, accuracy, clinical, decision, decision-making, human, acceptable, use, document, EHR