

AHRC NYC AI Use Policy:

Purpose and Scope

This policy outlines responsible practices and guidelines for AHRC NYC employees utilizing artificial intelligence (AI) technologies to assist in and for the purposes of developing service recording, documentation, and attestation, with a strict focus on safeguarding information protected by privacy laws.

The primary focus is to ensure the protection and privacy of all data that may contain protected health information (PHI), protected via HIPAA, student data, protected via FERPA and all personally identifiable information, (PII), of AHRC NYC stakeholders including but not limited to people supported, their families, staff, directors, contractors and donors.

This policy applies to all AHRC NYC stakeholders including staff, trainees, interns, volunteers, consultants, business associates, contractors and subcontractors as well as the Board of Directors, and particularly addresses composing any/all service recordings for People Supported.

1. Protection of Protected Health Information (PHI) and HIPAA Compliance

AHRC NYC is committed to maintaining the confidentiality and privacy of all "Persons Supported." To ensure full compliance with the Health Insurance Portability and Accountability Act (HIPAA) and other applicable regulations, the following guidelines must be observed:

- **Strict Prohibition on PHI in AI Platforms:** Under no circumstances should any identifiable information, including but not limited to names, medical histories, or service records of any Person Supported, be uploaded, shared, or processed through any AI technology, including AI-powered transcription, summarization, or analytical tools.
 - **Encryption and Data Anonymization:** Where AI tools are used to analyze or assist in generating service notes, employees must ensure that any datasets are anonymized and stripped of any identifiers before usage. This applies even if the AI technology provider claims encryption or privacy safeguards; AHRC NYC mandates a zero-PHI policy in all AI interactions.
 - **Additional Protection for Personally Identifiable Information (PII):** AHRC NYC further requires that all personally identifiable information (PII) pertaining to Persons Supported and employees must be safeguarded to the highest standards. Employees, contractors, interns and volunteers are prohibited from using AI tools to process PII, including but not limited to Social Security Numbers, addresses, or employment records.
-

2. FERPA Compliance

As an organization that provides services to students, AHRC NYC recognizes its responsibility to comply with the Family Educational Rights and Privacy Act (FERPA). The following measures are mandatory:

- **Strict Confidentiality for Student Records:** Any AI technology used to assist in educational documentation or communication must not process or store any information classified as an education record under FERPA.
 - **Training for FERPA Compliance:** Employees working in our education department must receive training on FERPA requirements to ensure that AI-assisted documentation respects the privacy and confidentiality of students and their families.
 - **Prohibited Use of AI for Educational Records:** AI tools may not be used to generate, analyze, or process records that contain identifiable information about students unless express authorization has been granted by the agency privacy office, and compliance safeguards are in place.
-

3. New York State SHIELD Act Compliance

AHRC NYC acknowledges its obligations under the New York State SHIELD Act to protect the personal identifiable information, (PII), of supported people, their families, employees, contractors, and donors. The following practices are required:

- **Data Security Safeguards:** No identifiable information pertaining to any agents of AHRC NYC (Employees, Contractors, Vendors, Interns, The Board, Volunteers, Donors) should ever be uploaded to any AI Tools.
 - **All Agents of AHRC NYC:** All Agents of AHRC NYC: must ensure that AI technologies do not process or analyze any sensitive data related to personal identifiable information, including but not limited to financial information or social security numbers. All such data must be de-identified in accordance with the SHIELD ACT and HIPAA standards and pre-approved by AHRC NYC's Security and Privacy office. **Incident Reporting:** Any suspected breach of data security involving AI tools must be reported immediately to AHRC NYC's **Privacy Officer** and **Security Officer** to ensure compliance with SHIELD Act reporting requirements.
-

4. Ethical Use and Practices Aligned with AHRC NYC's Mission

AHRC NYC is dedicated to ethical practices that support its mission to enhance the lives of the people it serves. AI technologies must be used in a manner that aligns with this commitment:

- **AI to Enhance Lives:** Employees are to use AI in ways that meaningfully enhance the quality of services provided to Persons Supported, prioritizing dignity, respect, and empowerment.
- **Transparency and Fairness:** Any AI tools used must operate transparently and without bias, ensuring equitable outcomes for all Persons Supported.

- **Promoting Human-Centered Approaches:** AI should complement, not replace, human judgment in decisions affecting the people AHRC NYC supports.
-

5. Verification of Information and Supervisor Signature Attestation

The accuracy, validity, and authenticity of all service recordings and attestations are of utmost importance to AHRC NYC. To maintain high standards of integrity and accountability, employees are expected to follow these practices:

- **Role of the Employee in Verification:** Employees play a critical role in ensuring the quality and integrity of service documentation, particularly when AI tools are involved. The responsibilities of employees include:
 - Carefully review all AI-assisted documentation for accuracy and completeness before entering any system and/or adding to a person supported chart.
 - Manual Cross-Check AI-generated content with source materials (e.g., session notes, direct observations) to ensure consistency and avoid discrepancies.
 - Take extra care to anonymize sensitive data before interacting with AI tools.
 - Stay updated on organizational policies regarding AI use and participate in training to enhance verification skills.
 - **Role of Supervisor in Verification:** A supervisor's signature on any document related to Persons Supported serves as a formal attestation of the document's content. By signing, the supervisor affirms that the information has been thoroughly reviewed, validated, and confirmed to be as accurate and complete as possible.
 - **Attestation Responsibility:** All employees must understand that their signature and that of the supervisor indicates their verification not only of the factual content but also that due diligence has been exercised in ensuring that no protected or sensitive information has been shared improperly or without authorization.
 - **Clear Documentation Process:** All employees are encouraged to follow AHRC NYC's documentation protocols diligently, especially when AI technology is involved in supporting the process. Supervisors should pay particular attention when any AI assistance is used, taking extra steps to confirm that no PHI or identifying details have been unintentionally disclosed.
-

6. Training, Compliance, and Reporting

AHRC NYC is dedicated to equipping employees with the tools and knowledge necessary for compliant and effective use of AI in their roles.

- **Mandatory Training:** All employees utilizing AI technologies for documentation purposes must complete AHRC NYC's data privacy and AI compliance training. This training will cover

best practices for AI use, HIPAA requirements, FERPA compliance, SHIELD Act obligations, and methods to avoid inadvertently disclosing sensitive information.

- **Incident Reporting:** If an employee suspects or identifies that sensitive information has been mistakenly uploaded, processed, or compromised in any AI system, they are required to report the incident immediately to the **Privacy Officer** and **Security Officer**. Timely reporting is critical to initiate remedial actions and ensure continued protection.
 - **Policy Violations:** Failure to adhere to this AI Policy may lead to disciplinary action, up to and including termination of employment. Employees are responsible for understanding and complying with this policy and should reach out to supervisors or the **Privacy Officer** and **Security Officer** with any questions or concerns.
-

7. Policy Updates

AHRC NYC will regularly review and update this policy as AI technology, regulatory requirements, and organizational needs evolve. Employees will be notified of significant policy changes and may be required to undergo additional training if necessary.

8. Unauthorized AI Note-Capturing Tools

To safeguard against potential breaches of protected health information (PHI) and personally identifiable information (PII), the use of third-party AI-powered note-taking or transcription tools during conference calls is strictly prohibited without prior approval.

- **Approval Process:**
Any request to use such tools must be submitted to the IT and Compliance Departments for review and approval. Requests must include:
 1. A description of the tool and its intended use.
 2. Documentation of the tool's data security and privacy measures.
- **Mandatory Orientation:**
Employees requesting approval for these tools must complete AHRC NYC's AI Use Case Orientation to ensure understanding of data privacy and security risks.
- **Reporting Unauthorized Use:**
Any employee who becomes aware of unauthorized use of AI tools during conference calls must report the incident immediately to the Privacy Officer and Security Officer.

This addition would help close any gaps in the policy related to real-time data capture during collaborative discussions.

9. Authorized AI Platform Usage: Microsoft Copilot Only

In alignment with AHRC NYC’s ongoing commitment to data security, regulatory compliance, and responsible technology use, the organization has designated **Microsoft Copilot** as the only authorized generative AI platform for internal use. This designation is based on Microsoft Copilot’s adherence to industry-leading compliance, privacy, and security standards, including HIPAA, FERPA, and the New York State SHIELD Act.

The following provisions apply:

- **Exclusive Use Requirement:** Microsoft Copilot is the only generative AI platform authorized for use by AHRC NYC employees, contractors, volunteers, or any other agents when AI assistance is needed in the editing, drafting, or development of service notes or documentation involving or related to Persons Supported.
- **Prohibited Platforms:** Use of any other generative AI platforms (e.g., ChatGPT, Google Gemini, Anthropic Claude, or others) for purposes related to documentation of services, note preparation, or interaction with any organizational data is **strictly prohibited**.
- **Data Safeguards within Copilot:** Although Copilot is authorized, employees must still comply with all privacy safeguards outlined in this policy, including anonymizing data wherever possible and never including PHI or PII directly unless expressly permitted by AHRC NYC’s Privacy and Security Officers under controlled conditions.
- **Compliance Monitoring:** AHRC NYC’s IT Dept. will monitor usage of AI tools to ensure adherence to this policy. Unauthorized use of any generative AI platform other than Microsoft Copilot may result in disciplinary action, including potential termination.
- **Training and Support:** All personnel utilizing Microsoft Copilot are required to complete designated training modules covering responsible use, privacy protocols, and secure integration into documentation workflows.

Acknowledgment

By using any AI technology within the scope of AHRC NYC’s operations, employees agree to adhere to the principles set forth in this policy and commit to the responsible use of AI technologies.

(Employee Name)

(Signature)

(Date)