

GEOCODE 489303

Continuum of Care Policies and Procedures

AI USAGE POLICY

ECHO WEST TEXAS

TX-625 LUBBOCK COUNTY & CITY COC

TX-625 Lubbock County & City Continuum of Care

Ending Community Homelessness Organization of West Texas

2005 Ave. T | Lubbock, Texas 79411 | 806.805.2762 | www.echotx.org

1. Introduction..... 3
 1.1. Purpose..... 3
 1.2. Scope..... 3
 1.3. Definitions..... 3
2. Policy Statements..... 4
 2.1. Prohibition of Sensitive Data Input..... 4
 2.2. AI Notetakers and Transcription Tools..... 4
 2.3. AI Chatbots..... 4
 2.4. Permitted Use of Aggregated or Anonymized Data..... 4
 2.5. User Responsibilities..... 4
3. Enforcement..... 4
4. Exceptions..... 5
5. Related Policies..... 5
6. Contact..... 5

date??	Initial document release
--------	--------------------------

1. Introduction

1.1. Purpose

Artificial Intelligence (AI) offers powerful new capabilities for analyzing and interpreting data, improving efficiency, and improving outcomes for those we serve. When applied to aggregated, non-identifiable information, the use of AI is encouraged to enhance productivity, decision-making, and insight generation.

However, the input or processing of non-aggregated, sensitive client data in AI environments presents significant risks, including potential privacy violations, regulatory non-compliance, and data breaches. This policy sets forth clear guidelines and restrictions to ensure that AI tools are used responsibly, and that client confidentiality and data protection standards are maintained at all times.

1.2. Scope

This policy applies to all persons handling sensitive client data collected from, or for input into, the ECHO Community Database/HMIS, including but not limited to - employees, contractors, vendors, participating agencies, and additional third parties who use AI tools or platforms, which include:

- Generative AI platforms (e.g. ChatGPT, Google Gemini, Microsoft Copilot)
- AI notetakers and transcription services (e.g. Otter.ai, Fireflies.ai, Zoom AI Companion, Microsoft Teams Copilot)
- AI Chatbots (internal or third-party)
- Any AI system capable of recording, transcribing, generating, analyzing, or storing client-related information

1.3. Definitions

- 1.3.1. **Sensitive Client Data:** Information that identifies or could reasonably be used to identify a client, including but not limited to names, contact details, account numbers, financial data, health information, personal identifiers (i.e. SSNs), or any data subject to data privacy regulations.
- 1.3.2. **Non-Aggregated Data:** Data that is raw, individual-level, or has not been anonymized or aggregated in a way that prevents the identification of the client.

- 1.3.3. **AI Environment:** Any system or platform that uses machine learning, natural language processing, or other forms of AI to generate, process, or analyze data.

2. Policy Statements

2.1. Prohibition of Sensitive Data Input

No non-aggregated, sensitive client data **shall not be** entered, shared, uploaded, or otherwise disclosed in any AI environment.

This includes manual input or automatic capture via voice, transcription, or screen recording tools.

2.2. AI Notetakers and Transcription Tools

AI Notetakers **must not be** used during any meeting, call, or virtual session where sensitive client data is discussed. Refer to **section 4** for Exception Requests & requirements

2.3. AI Chatbots

Use of sensitive client data within a generative AI environment that includes a “Chatbot”, refer to **section 1.2** for examples, **is expressly prohibited** due to the nature of the current AI Chatbot environments - how data is stored and how the data can potentially be leaked as a result of queries from outside parties.

Any interaction with an AI Chatbot must be limited to aggregated or Anonymized Data.

2.4. Permitted Use of Aggregated or Anonymized Data

Only fully anonymized or aggregated data may be used in AI environments not explicitly approved by the CoC Database Committee and CoC Board.

2.5. User Responsibilities

Users must not circumvent this policy by intentionally masking data or using abbreviations to avoid detection. All users must complete annual training on AI risk, responsible use, and client data protection as part of their required annual security and data protection training.

3. Enforcement

Violations of this policy may lead to revocation of access to the ECHO Community Database/HMIS for an individual or entire organization. Violations that result in unauthorized access or leaking of sensitive client data to unauthorized persons may also result in a referral to law enforcement authorities for investigation with the full cooperation of the CoC Board of Directors and ECHO West Texas.

4. Exceptions

In the event an agency or organization can establish a business need and justification for the use of an AI tool in conjunction with client level data, an Exception Request may be made.

Exception requests must be submitted in writing to ECHO West Texas and include:

- Description of intended AI tool and use case
 - **Only** AI tools that are HIPAA compliant will be considered. All others will be rejected outright.
- Nature and classification of the data involved
- Justification and business need
- Proposed controls and safeguards

Approval must be granted by the CoC Database Committee **and** CoC Board of Directors before proceeding with the use of an AI tool.

5. Policy Review

This policy will be reviewed by the CoC Database Committee at least once a year and as needed with changes in the AI and business landscape.

6. Related Policies

- HMIS/Database Policies & Procedures
- Contributory HMIS Organization Agreement
- HMIS End User Agreement
- HMIS Privacy Notice
- HMIS Release of Information
- HUD 2004 HMIS Data and Technical Standards Final Notice
- HUD 2004 Security Notice

7. Contact

For clarification, training, or exception requests, contact:

ECHO Database Administrator:

data@echotx.org