Linea Solutions

Artificial Intelligence (AI) Data Security Policy:

Protecting Sensitive Data when Using AI

November 2023

Version 1.0

Linea Solutions
lineasolutions.com

4551 Glencoe Ave. Suite 140
Marina del Rey, CA 90292

P 310.331.8133
F 310.807.4356

Table of Contents

Table of Contents

Document Information

Revision History

Version	Author/Reviewer	Description of Change	Date
0.1	Beth Haught	Initial draft	3/23/2023
0.2	Nate Haws	More AI specialized expertise	3/24/2023
0.3	Beth Haught	Incorporated feedback from Akio and Nathan	4/12/2023
0.3	• Beth Haught • Matthew Hathaway-Bates • Idrissa Davis • Jason Todd	Linea Technology Leadership Review	5/1/2023
0.4	Beth Haught	Incorporated comments from review and updated with User Data Opt Out instructions	5/20/2023
0.5	• Akio Tagawa (Approve) • Peter Dewar (Review) • Kim Zierath, Implementation Consulting (Review) • Angela Li, Pension Consulting (Review) • Wayne Ellis, Insurance Consulting (Review)	Linea Management Leadership Review	5/19/2023
0.6	Gillian Major	Updating Safe Practices following Claude2 policy and added additional items for acceptable use policy at a general level.	8/23/2023
0.7	Nate Haws	Incorporating more tools beyond OpenAI	8/26/2023
0.8	Gillian Major	Making the policy more tool-agnostic and added general guidelines.	9/20/2023

Version	Author/Reviewer	Description of Change	Date
0.9	Gillian Major	Reformatted tool summary into chart format and added additional chart.	9/25/2023
1.0	Nate Haws	Approved	11/9/2023

Approval

Version	Approver	Organization	Approved
Artificial Intelligence (AI) Data Security Policy: Protecting Sensitive Data when Using AI			
	Akio Tagawa, Principal	**Linea Solutions**	10/11/2023
	Peter Dewar, President	**Linea Secure**	10/11/2023

Introduction

Purpose

This policy defines the general goals and procedures necessary to ensure that Linea Solutions protects our own data as well as client's data while utilizing Generative AI tools, specifically Large Language Models (LLM). LLMs can potentially capture and retain input and output data for ongoing use by the LLM. As a result, careful consideration should be given about whether LLM tools should be used, given the data that will be submitted. For the purposes of this document, "Linea" means Linea Solutions and all its affiliated companies.

Scope

The scope of this policy is to guide the use of any Generative AI tool, such as OpenAI's ChatGPT Plus or Anthropic's Claude, for Linea internal and client work to protect Linea and client data assets.

Background

Multiple Generative AI large language models (LLM's) have become publicly available in recent months. These models are accessed via various interfaces/tools that Linea employees can use to improve efficiency in internal and client facing work. This section provides some background information about each of these models and guidelines for using their various interfaces. **Depending on the tool's privacy policy, the cleaning of sensitive data [specifically client identifying data like client names and performance, weaknesses, threats, vulnerabilities etc.], is or isn't required of employees by Linea's AI Policy.** Though, whether client identifying data needs to be scrubbed or not, the submission of any personally identifiable information (PII), personal health information (PHI), or Linea proprietary information (PI) to a Generative AI tool is strictly prohibited.

AI Tools Overview

The table of AI tools listed below provides a list of vendors and tools that Linea may use for every day productivity and/or client facing work. The table also describes the type of tool and whether or not any client identifying information should be scrubbed from data submitted to the tool.

Vendor	Tool	Type	Data Cleaning Required?
ChatGPT	ChatGPT Plus	LLM Chatbot (with chat history disabled)	No
	ChatGPT Plus	LLM Chatbot (with chat history enabled)	Yes
	Playground	Configurable LLM Chatbot	Yes
	API	Application Programming Interface	No
Anthropic	Claude Pro	LLM Chatbot	No
	API	Application Programming Interface	No
CustomGPT	CustomGPT.ai	Custom-Dataset-Trained LLM Chatbot	No
Atoma	Patterns	Custom AI Application Development Tool	No

Privacy and Security

OpenAI's ChatGPT Plus with chat history disabled, for example, is one of the tools that Linea recognizes was being very safe as their privacy policy is relatively iron-clad. When assessing a tool's policy, Linea is looking for specific markers that convey safety around the inclusion of client identifying information. As noted in the above chart, the same goes for Anthropic's Claude Pro - scrubbing of client-specific information is not required.

For a more detailed review of how Linea accesses the safety of AI tools, refer to subsection "AI Data Security Process."

Third-Party Custom Generative AI Chatbot Vendors

Third-party custom generative AI chatbot vendors use generative AI LLM's APIs to essentially train a LLM by uploading a custom data set, indexing this data with semantic embeddings, and storing the embeddings in a vector database. These custom-trained models can serve as knowledgebases for organizations, clients, etc. and they will treat their training data like the facts and minimize hallucinations.

The custom LLM chatbots that is currently approved for Linea use (CustomGPT.ai) is a third-party vendor and is presently SOC2 **pending**, thus some clients may be hesitant to approve this tool for client use. However, if training data does not include PII, PHI or PI, then they may make an exception. CustomGPT.ai is Linea's preferred custom chatbot vendor.

AI Tools for Meeting Summarization

Linea currently uses generative AI to create meeting summaries, specifically **Linea uses Teams' Intelligent Meeting Recap** for Teams meetings. This tool requires that meetings be recorded, thus potentially introducing privacy risks if sensitive information is discussed in the recording. Care should be taken in granting access and monitoring data practices.

Intelligent Meeting Recap for Microsoft Teams

Microsoft's Intelligent Meeting Recap is fully integrated into Teams. Since September 2023, Linea has transitioned into sole use of this tool, which operates as such:

- Auto-generates a summary of every meeting via the processing of the meeting's transcript.
  - Leverages speech recognition and NLP capabilities to make said transcript.
- Does not store meeting recordings but does store meeting transcripts.
- Has all of the same security and compliance standards as Microsoft.
  - Requires trust in Microsoft for any meeting data processed through Teams.
- Has limited compatibility to meetings run via Teams.

Fathom for Zoom

Linea no longer uses Fathom, a third-party plugin for Zoom, to create AI-generated meeting summaries. Though, some clients might be unwilling to meet via Teams, thus Fathom can be used in those cases.

Policy

Rules of Engagement

1. Use of Generative AI tools must adhere to this policy.
2. Linea employees must first get approval from
   - The **Engagement Manager (EM)**, when using any AI on project work.
   - The **AI Governance Committee**, when using any AI on corporate research, development, or training work.
   - The **affected client**, when using OpenAI, Anthropic, third party custom Ai chatbots or AI meeting summary tools with client-specific data.

3. Before using ChatGPT's interface for business purposes, Linea employees must set their "Chat history & training" off under the data controls settings.
    - Sidenote: Keeping one's "Chat history & training" turned on can allow for the leveraging of many high quality features. For example, when maintaining long-term conversations with ChatGPT, one enables the model to build its own context/understanding of your project and its own memory of your prefered tone, style, etc. This can greatly increase the quality of ChatGPT's responses.
    - **If a consultant wants to turn on their chat histroy, they'll need to get approval from the project's EM**.
4. When using custom AI chatbots, ensure that the base prompt informs users that they are interacting with an automated AI system.

Turn off Chat History & Training

Follow these instructions to turn your "Chat history & training" in ChatGPT off/on:

1. Open a ChatGPT session.
2. To the bottom left of the chat, click on your email.
3. Then click "Settings" > "Data Controls."
4. Toggle off [or on] "Chat history & training."

Generative AI Usage Policy

1. **Do not rely on OpenAI, Anthropic, Custom AI Chatbots, or any other AI output to be error free**. Social biases, hallucinations, and adversarial prompts are a threat to quality, client-worthy output. All AI-generated output is to be consultant-reviewed prior to delivery.
2. **Obtain approval prior to using OpenAI, Anthropic, Custom AI Chatbots, or any other AI for client work**. Before using AI for any client work, consult this policy, discuss with your EM, and gain client approval if applicable.
3. **Recognize limitations prior to using OpenAI, Anthropic, Custom AI Chatbots, or any other AI.** When using OpenAI technologies with client-specific content, the API Content software must be used based on these terms of service:

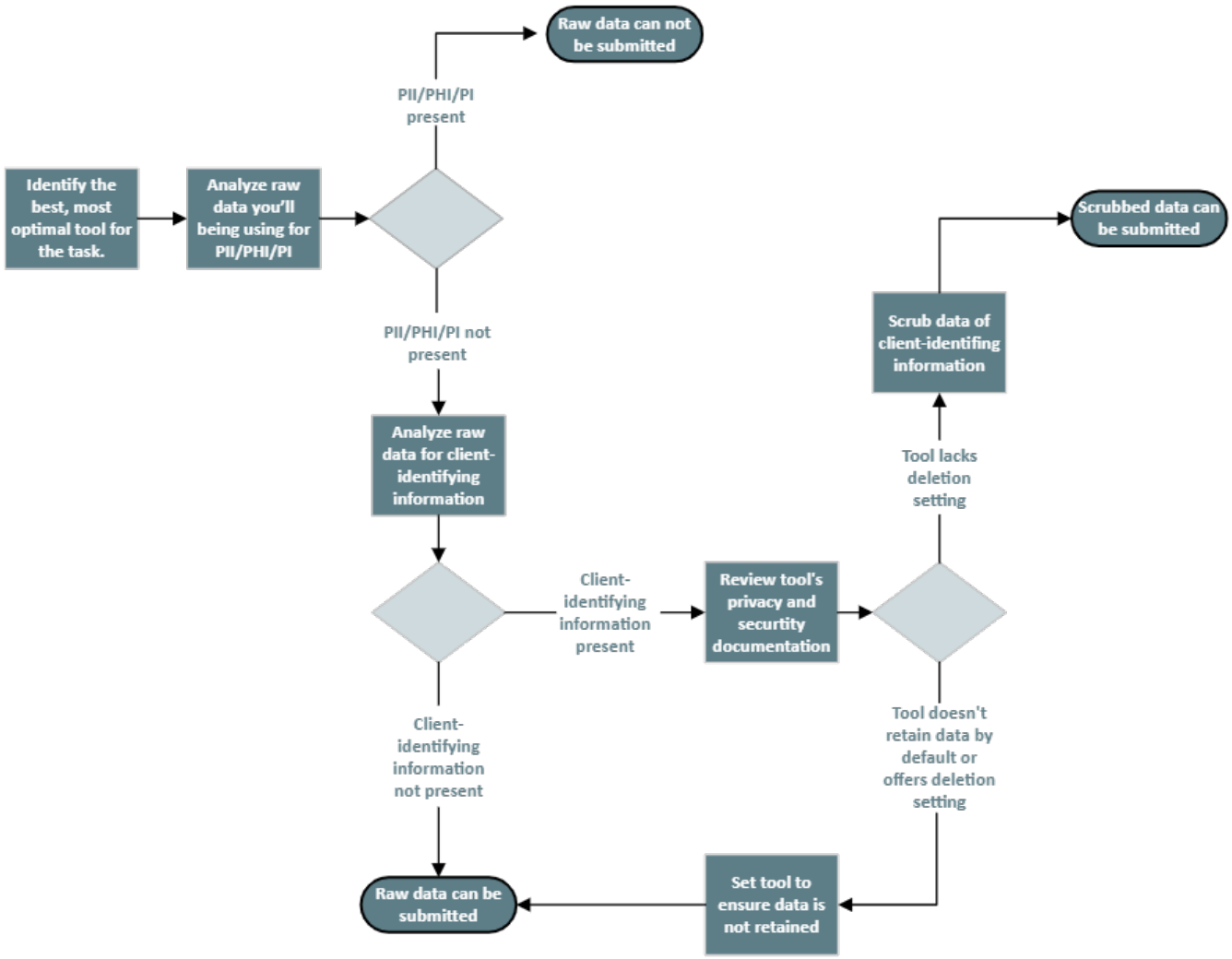
    > *(c) Use of Content to Improve Services. We do not use Content that you provide to or receive from our API ("API Content") to develop or improve our Services. We may use Content from Services other than our API ("Non-API Content") to help develop and improve our Services*

4. **Using OpenAI, Anthropic, Custom AI Chatbots, or any other AI for general research.** When using AI for general research (e.g. market research, learning), a multitude of interfaces can be used. If research involves client work, ensure the proper information is scrubbed from one's data/prompt as stated in the "Background" chapter of this policy.
5. **Using APIs for general research**. Using, for example, OpenAI's API for general research can increase data security. It is still best practice to remove certain information from one's data/prompt as stated in the "Background" chapter of this policy

6. **"Human-in-the-loop" implementation at the client level.** Ensuring that the client is always "in-the-loop" permits project staff/LOB users to review given information. As mentioned, for example, if AI (like a custom chatbot) is client- or member-facing, a disclosure should auto-populate to inform the user that all answers are sourced from AI.

AI Data Security Process

The following diagram maps out Linea's protocol for properly assessing a tool's privacy and security settings against the kind of data employees might be handling when leaning on an AI tool for a task or project.



As listed, **the key to using AI at the workplace is knowing what kind of data you are working with**. That is, whether or not the data has PII, PHI, or Proprietary Information (PI) present, and secondly

whether or not the data contains client-identifying information. From there, it is up to your tool's own privacy and security documentation to necessitate proper data scrubbing prior to use of the tool.