Smart Scribe JotPsych

Authored: July 8, 2024
Updated: July 8, 2024

SmartScribe Corp. transcribes audio using AssemblyAI, a SOC 2 Type 1 & Type 2 compliant audio transcription provider which redacts personally identifiable information (PII) from transcripts.

What is SOC 2?

SOC 2 (Service Organization Control 2) is a framework for managing customer data based on five "trust service principles"—security, availability, processing integrity, confidentiality, and privacy. Compliance with SOC 2 is essential for any organization that handles customer data, ensuring that systems are designed to keep sensitive information secure. SOC 2 compliance is evaluated through two types of reports:

SOC 2 Type 1

- **Definition**: SOC 2 Type 1 reports evaluate the design of security processes and controls at a specific point in time. It assesses whether the system and organizational controls are suitably designed to meet the relevant trust service principles as of a specific date.
- **Focus**: The focus is on the design and implementation of the controls, providing a snapshot of the organization's control environment at the time of the audit.
- **Purpose**: This type of report is typically used by organizations to demonstrate that they have the necessary controls in place to protect customer data, even though the effectiveness of these controls over time is not assessed.

SOC 2 Type 2

- **Definition**: SOC 2 Type 2 reports evaluate the operational effectiveness of the security processes and controls over a period of time, usually a minimum of six months. It assesses not only the design of the controls but also their consistent and effective operation.
- **Focus**: The focus is on the ongoing effectiveness of the controls in place, providing a historical perspective of how well the organization has adhered to its control processes.
- **Purpose**: This type of report is more comprehensive and is used to provide assurance to customers that the organization's controls are not only properly designed but also operating effectively over time to protect customer data.

To learn more about AssemblyAI's SOC 2 compliance, click here.

What is PII?

Personally Identifiable Information (PII) refers to any data that can be used to identify a specific individual. This includes, but is not limited to, names, addresses, social security numbers, email addresses, phone numbers, and any other information that can be linked to an individual. Protecting PII is crucial for maintaining privacy and security.

What is PII Redaction?

PII Redaction is the process of removing or obscuring personally identifiable information from documents and datasets to prevent unauthorized access and misuse. This process ensures that sensitive information is not disclosed inappropriately, while still allowing the remaining data to be used for its intended purposes.

Key Elements of PII Redaction:

1. **Identification of PII**: The first step in the redaction process is identifying all instances of PII within a document or dataset. This includes not only obvious identifiers like names and social security numbers but also indirect identifiers that, when combined, could be used to identify an individual.

2. **Redaction Methods**: Various methods are used to redact PII, including:
    - **Manual Redaction**: Human reviewers manually go through documents to find and redact PII.
    - **Automated Redaction**: Software tools scan documents and datasets to automatically identify and redact PII using predefined algorithms and rules.
3. **Validation**: After redaction, it is essential to validate that all PII has been correctly and completely redacted. This step often involves both automated checks and manual reviews to ensure accuracy and completeness.
4. **Security Controls**: Implementing security controls to manage access to unredacted information is critical. Only authorized personnel should have access to original documents containing PII, and strong access control measures should be in place to prevent unauthorized access.

Importance of PII Redaction:

- **Compliance**: Many regulations and standards, such as GDPR (General Data Protection Regulation), HIPAA (Health Insurance Portability and Accountability Act), and CCPA (California Consumer Privacy Act), require the protection of PII. Redaction helps organizations comply with these regulations.
- **Privacy Protection**: Redacting PII helps protect individuals' privacy by ensuring that sensitive information is not exposed to unauthorized parties.
- **Risk Mitigation**: By removing or obscuring PII, organizations can reduce the risk of data breaches, identity theft, and other malicious activities.

To learn more about AssemblyAI's process of ensuring PII Redaction, click here.