Oloid AI

Data Security and User Privacy Framework

Operating principles, architectural design and best practices implemented by Oloid that provides a strong assurance of data security and privacy

—

Oloid Inc.
440 N Wolfe Rd
Sunnyvale, CA 94085
www.oloid.ai

Background

Whilst data, big data and data sets are becoming increasingly used by companies to inform managerial decisions, workers' data protection and privacy are still evolving.

Oloid is committed to protecting all information relating to its customers and users, as well as protecting its confidential business information (including information relating to its employees, affiliates, and members). To achieve this goal and to minimize the risk of loss, theft, or compromise of business or PII-related information, appropriate systems, operating procedures, and policies are in effect and are regularly reviewed and updated.

This document provides an overview of the operational principles, architectural design and best practices implemented by Oloid that provides a strong assurance of data security and privacy of employee data.

Operating Principles

Following are the general principles followed by Oloid for ensuring data privacy and protection:

1. **Consent**
   - Users must have access to, and influence over, data collected on them
   - The platform/technology should leverage the existing consent framework of the customer (employer/employee/contractor/visitor contracts and policies)
   - The data collection, retention and purge policies should conform to the local regulations and guidelines
2. **Encryption and Data Processing Safeguards**
   - All external connections to and from production system to be through https with SSL/TLs certificate. Internal connections to production system can only happen through VPN.
   - All data storage on cloud infrastructure (data at rest) is encrypted at AES 256 or comparable standards.
   - ITIL processes and appropriate legal/confidentiality agreements for ensuring access control of data
   - Anonymization of data for analytics and reporting, wherever identification is not required
3. **Proportionality and subsidiarity**
   - Data collection must be limited to what is necessary to achieve the objectives of the collection in question
4. **Transparency**
   - Information concerning personal data held by employers must be made available to the employee directly or through an intermediary upon a disclosure request
   - Users should be informed if material changes are made to the data management policies

5. **Conformance to Privacy Laws**
    - Comply with the federal and regional requirements, regulations and guidelines on data rights and privacy
    - Redressal process and contact for addressing requests for data disclosure e.g. GDPR requests, CCPA requests

Privacy by Design (Architecture):

Oloid has made several design choices to apply the above principles:

1. **Data Minimization**
    - Oloid stores wellness attestation (responses to questions about symptoms and travel history) inside the QR code itself and the data is not transmitted to Oloid or the employer until the QR code is used
    - The QR code for wellness attestations can be setup to expire after a defined period at which point the data cannot be extracted by Oloid or the employer
2. **De-identification**
    - For facial authentication (contactless biometrics), the facial picture is converted into a numeric bit. Subsequently the bit sequence is primarily employed for authentication
3. **Data Auto Deletion/Purge**
    - When the user uses the QR code to provide attestation data at entry points, the data is automatically purged from the Oloid system
    - The user data (images and activity data) submitted in Oloid's demo application is automatically deleted every 24 hours

Health Information Privacy

While Oloid's products are not meant to deliver a medical service, the wellness attestation application may capture responses about health symptoms and/or skin temperature. Specifically, when using thermal scanning, the assessment of normal or elevated skin temperature could be deemed as data that needs to be treated as private health information.

Oloid helps organizations stay compliant with such health information privacy requirements by providing features/capabilities that protect the privacy of the users:

1. **No Loud Audio or Prominent Visual Alerts**
    - Certain systems rely on a loud alarm or a beeping buzzer to draw attention towards an individual who may be identified at-risk either as a result of the responses to the wellness questionnaire or as a result of elevated skin temperature. Such loud alarms can be easily heard by other individuals in the vicinity. Not only is such identification of "at-risk" determination an imperfect science and at best indicative, even if an individual were to be

truly "at risk" such information needs to be handled sensitively. A broadcast of such information could shame such a person and in certain circumstances deemed as violation of that individual's health information privacy rights protected under HIPAA

- Other systems employ prominent red or green lights that indicate the "at risk" status. Similar to the above point regarding loud alarms/buzzers, such indications can also have similar considerations from health information privacy standpoint.
- Oloid provides a very subtle visual feedback which is designed to be only visible to the user. Additionally, the sound can be turned off on the device to ensure auditory and visual privacy of the user

2. **Access Control for Data**
   - Organizations may find it useful to retain the collected wellness attestation form data and the elevated skin temperature screening results as an audit trail and for contact tracing purposes
   - Oloid lets the organization control who has access to the collected wellness attestation form data and the elevated skin temperature screening results
   - The organization can determine on a per device/entry level, who would be recipient of the data and/or alerts; this can be an individual or a group/alias comprising of multiple individuals
   - Additionally, if the organization does not want any named individual to have access to the data, the organization IT team can create an email address ehs@companyname.com and the data can be transferred to this account. The IT access controls of this account will determine the access control of the data

3. **Data Deletion/Purge**
   - When the user uses the QR code to provide attestation data at entry points, the wellness attestation form data and the elevated skin temperature screening results are pushed into the company's servers and data is automatically purged from the Oloid system
   - The wellness attestation form data and the elevated skin temperature screening results which is pushed into the company's servers can be setup by the organization's IT team such that the data is automatically purged from the email account every 30 days or whatever period is deemed adequate for audit and contact tracing as per the organization's policies