Aira Security and Privacy Whitepaper

Date: 8/4/2017, V2.10

The purpose of this document is to describe the policies, controls and procedures Aira uses to reduce the risks and threats to the users, corporations, organizations and schools who use the Aira Service.

Introduction

Aira is a service that enables users to more fully embrace the moments of their lives and achieve greater autonomy through cutting edge technology. By combining Aira provided Smart Glasses and MiFi with user cell phones, our customers are ready to further experience and explore the world with a new perspective.

The remote assistance platform that connects Aira Trained Agents to customers follows a very strict set privacy and security policies. The video, audio, and sensor data can contain personal or corporate data, and therefore is handled with the utmost care. The connection and trust between our users and Aira drives our culture and in turn our- mindset towards privacy and security. To ensure the quality of service we provide, the Aira team is required to go through extensive training. This training is the cornerstone of our relationship with our users.

This paper describes Aira's approach to security, privacy, and compliance. In this document you find details about how our offering keeps information safe and maintains the highest levels of service.

Glossary of Terms

Term	Definition
AES	The de facto algorithm used to encrypt TLS communications. It stands for Advanced Encryption Standard.
Agent	A contractor or an employee of Aira, who is legally bound by our confidentiality agreement to keep user information private, that directly assists the user.
Agent Dashboard	An proprietary tool that agents use to assist users. It contains the real time data such as video, audio, gps, sensors etc. within an easy to user dashboard interface.
Analyst	An employee of Aira who supervises a specific team of Agents
AWS	Amazon Web Services

Component	One of many special purpose/functional units that when combined form our platform
DevOps	A clipped compound of “development” and “operations”. It refers to the transition process of taking developed software and deploying it to a production or production-like environment.
DTM	LTE high priority, private network provided by AT&T, called Dynamic Traffic Management
Hotspot	Wireless access points providing network and/or Internet access to mobile devices like your laptop or smartphone.
LTE	A standard for high speed wireless telecommunication (4G). It stands for Long Term Evolution.
MiFi	A wireless router that acts as a mobile WiFi Hotspot
PCI	Payment Card Industry
Platform	The software infrastructure that exists in the cloud that is responsible for service operations
Service	The enabling of Users to navigate about their business through Aira technology with the collaboration of an agent.
Smart Glasses	Wearable computer glasses typically equipped with camera, sensors, and a tiny computer that add information alongside or to what the wearer sees.
Smart App	Innovative systems that gather tremendous amounts of data from sensors and other sources, using machine learning algorithms and predictive analytics to make this information actionable for users and to improve experiences.
SSH	A protocol for secure remote login from one computer to another. It is commonly referred to as Secure Shell.
TLS	The latest cryptographic protocol that provides security over a computer network. It stands for Transport Layer Security.
User	An individual who is allowed by Aira to use the products and services provided.
VPC	AWS Virtual Private Cloud
Workforce	The employees, contractors, and agent contractors that compose Aira

Aira Has a Strong Security Culture

It is an intrinsic part of Aira culture to respect and understand the need to maintain user privacy while ensuring all information is secure. Many of it’s key executives and engineers have

previously worked at SaaS companies such as Intuit Inc., makers of TurboTax and Quickbooks, and come with a deep understanding of security, privacy and compliance. Through the rigorous hiring process, thorough testing, detailed onboarding, focused training, and continuous reviewing, all employees are acutely aware of their responsibility to keep Aira a safe place for our customers.

Agent screening and background checks

Applicants for agent, analyst, or customer service representative positions must have a minimum of 2 years prior relevant work experience. Over 70% of hires have at least a bachelor's degree for their education.

Before an applicant can join our agents, the individual must go through an 4 step process. First the person must answer the pre-screening questions designed to ensure an initial set of privacy and security concerns will be observed. After this initial screening, a test is conducted to ascertain aptitude and ability to perform the work according to company policy. Candidates are then scheduled and interviewed for background qualifications and personal skills. Successful candidates sign documents defining confidential information (including personally identifiable), how such information is to be handled, and validates the candidate's legal ability to work in the US.

After signing the documents a thorough background check is conducted to verify any and all criminal records. Background checks extend to all Aira employees and personnel including software development and finance.

Security training for all all Aira personnel

The entire Aira workforce undergoes security training as part of their onboarding; this in addition to the confidentiality agreement they sign. This training focuses on security and privacy concerns, as users may engage in activities that involve private/sensitive aspects of their life (bank statements, medicine labels, etc.). Personnel who regularly interact with users continue to receive training (beyond their initial 30 hours) and have their interactions subject to review. It is important to recognize that as part of the training for agents and analysts, they are taught to make the user aware of "privacy mode". This mode temporarily disables audio and video, such that the user can ensure a potentially sensitive situation is not shared. The user is in full control of when this mode is activated and when it is deactivated.

Our security team

All engineers and system architects are responsible for the security of our service. In this way, each person who contributes to the design and implementation of our service is a part of our security team. Each engineering effort, design, and code contribution is subject to a rigorous review which involves a security assessment. Because we leverage enterprise technologies which are continuously patched and hardened in addition to complying with various industry specific security policies, our platform reaps those benefits. To ensure that those security benefits are sustained, all Aira components are assessed to make sure they follow the standards set forth by the technology creator (ie. AWS is our cloud vendor and has a detailed listing of best practices for use with their technology https://aws.amazon.com/whitepapers/aws-security-best-practices/). We follow the best practices of all the technologies we leverage. Each technology is evaluated in advance for security compatibility with our existing infrastructure. Aira firmly believes in confirming our solutions genuinely solve the issues. Our penetration/vulnerability testing is a never ending effort that ensures our service is reliable and secure.

Internal audit and compliance

Aira continuously audits agent and user interaction for security and privacy policy adherence (as well as the general corporate policies). Agents regularly are reviewed including audit of their sessions by their supervising analyst. Analysts ensure proper procedure is followed at all times and if an irregularity is observed in a session, the analyst contacts the agent and addresses the issue . In addition to session review process there are Agent community meetings which serve as both a communal knowledge and experience share as well as further training over a myriad of different topics (including privacy and security practices designed to protect the user and any confidential information that may be came across). Aira recognizes that enterprise security is a continually evolving topic, and as such these community meetings serve as a platform to keep our agents and analysts aware of the latest trends. Our expert team of engineers and system architects ensure that our infrastructure is always up to date with the latest practices (for design) and the latest patches (for vulnerability fixes).

Monitoring

Aira's security monitoring takes numerous forms, from the Cloud Watch provided by Amazon to the platform logging. We regularly monitor our platform and subcomponents for irregularities both for performance reasons and to ensure no unscrupulous actions were attempted. In addition to authentication ensuring only valid requests/communications are accepted, we collect anonymous usage data. This anonymous usage is leveraged to not only fine tune performance but to also act as an additional safety net to identify atypical behavior within the system that can be investigated and responded to.

Technology with Security at Its Core

Aira's infrastructure runs on the global leading cloud platform, AWS. By combining their offering with our expert architecture, we're able to deliver privacy and security while maintaining the conveniences our customers have come to love.

Secure Platform Design

The multilayer security of the platform comes from the VPC within AWS and the TLS protocol that guards all internal and external communication. This ensures our network is not publicly accessible, and all traffic through our private network is secure with respect to our private network as well (via AES 256). The platform is an aggregation of special purpose components, with each component having its own security group. These security groups restrict both access and communication. The gateway acts as the front door to our VPC, and only allows our proprietary communication through (this prevents people from being able to leverage SSH to access servers within our VPC).

With respect to storage, we do not store any payment related information. All credit card related information is handled by Recurly, which is a PCI-DSS level 1 compliant vendor. We store basic profile information behind an Amazon Relational Database security and management system (which restricts access by IP among other criteria).

Secure Private Network for Customer Hardware

Our service leverages 3 hardware devices the user carries with them: their cell phone, our MiFi, and our Smart Glasses. The MiFi is an AT&T proprietary device that enables the user's communications via AT&T's DTM network (which the public does not have access to). Each MiFi restricts access not only by having a unique network name and unique password, it restricts the number of connected hosts to 2 devices. The Smart Glasses ship with the MiFi are already paired before the user receives it (thus eliminating the concern around the security associated with sharing access credentials).

Safe Communication and Distribution of Applications for Agents

Agents assist users by using our Agent Dashboard. It is important to note that before the Agent even gains access to dashboard, let alone attempts to download the application, the destination computer must meet the pre-approved specifications of hardware and software. The Agent Dashboard has a secure distribution via an internal tool which leverages authentication and authorization principles before providing the application for secure download. Our software is signed by Microsoft and Apple, such that they are valid when installed (if an agent were to be prompted about untrusted software installation that would

immediately flag the binary as invalid). When the application is run, all communication (audio, video, gps, etc.) is secured via TLS. All sessions are securely stored in our Cloud Platform. Each session has restricted access to prevent the dissemination of private information.

Securing data in transit

Aira ensures that all the data as it transmits from the user environment and flows through to our private network is always multilayer protected. The Smart Glasses not only encrypts the streaming video using the latest enterprise standard TLS, but it also ensures the transport is safely conducted through a personal MiFi device. The MiFi provides a local private network which routes the stream of encrypted data through AT&T's Dynamic Traffic Management (DTM) private LTE network until it reaches our Virtual Private Cloud (VPC). This over the air communication through DTM provides our customers with priority routing (which avoids user congestion through cell towers) and an additional security layer on top of the AES 256 encryption provided by the TLS. Once the data arrives at our VPC in Amazon, it goes through our exclusive gateway. All communication and routing within our VPC is TLS protected.

Low latency and highly available solution

Our guarantee to our customers is that communication from the time from the user streams the video until the agent assisting views the stream is always less than a second. These latency times a carefully monitored with more than 80% of the streams traversing the system in ⅕ of a second and 99% traversing the system in under ½ of a second. We complement this incredibly low latency with our high availability strategy. By leveraging AWS, we are guaranteed the platform will have a minimum uptime of 99.99% throughout the year. We are able to achieve this performance by having each component in the platform dynamically scale based on user demand.

Data Usage

Our philosophy

Aira maintains a user profile that contains the minimal amount of information needed to ensure safe and efficient interactions with the customer. Information such as quality of eyesight (e.g. low vision vs. fully blind), mobility aid (e.g. cane or guide dog) are collected and stored so the Agent can access and adapt their instructions during a session. No health or contact information are asked for. See full privacy terms here: https://aira.io/privacy-policy

The sessions that are recorded are solely viewed for the purposes of ensuring our agents' interactions are appropriate,to the high standards set forth in our training sessions, demonstrations of the technology and training internal algorithms to perform intelligently. Any other uses are strictly forbidden and requires executive level approval.

Data Access and Restrictions

Administrative access

Access to any files and/or applications within the platform is restricted. Access is exclusive to our DevOps professionals that are part of an access control list (which is restricted by IP in addition to credentials). A very exclusive list of employees have access to production and its data, which is under the direct review of management.

Conclusion

The convenient, safe, private, secure experience of our users is the primary concern of Aira. Every aspect of our business drives towards achieving the highest level of trust which depends on this platform of security and privacy. Only Aira can protect user data and meet the real time demands of a user's session. Because security is on the forefront of our thoughts, our users don't have to worry about it and can fully embrace the moment. For these reasons and more, new users come to Aira each day.