orbita

Secure Voice in Healthcare:

The What, Why, and How of HIPAA-Eligible Voice Assistants

INTRODUCTION

The success of smart speakers and voice assistants like Amazon Alexa and Google Assistant has inspired many to consider their potential as virtual assistants for digital healthcare applications. The idea is simple - provide the patient (or care provider) a natural, conversational virtual assistant that can streamline and automate common care tasks to improve quality of care and outcomes, while reducing costs.

In a survey published by Microsoft in April 2019, 41% of voice assistant users said they had concerns about privacy and security.

AI-powered virtual assistants, whether delivered over a smart speaker, or through a web or mobile chatbot, are the next "front door" in digital health. They can answer healthcare related questions, deliver care reminders, send messages, capture and retrieve healthcare data, schedule appointments, and perform many other tasks through the power of voice and conversational interfaces.

As the idea of voice and chat virtual assistants has gained steam in the healthcare industry, so has concern about personal data privacy and security. In a survey published by Microsoft in April 2019, 41 percent of voice assistant users said they had concerns about privacy and security. In healthcare, these concerns are amplified by the inherent sensitivity of personal health information.

Ensuring the privacy and security of personal information is already an imperative for anyone operating in the healthcare industry. Providers, payers, and other organizations that handle personal health data are bound by law to ensure that these data do not get mishandled or improperly exposed.

IN THIS WHITE PAPER:

- **Overview of HIPAA compliance for secure healthcare voice assistants**
- **Best practices for secure voice applications with Orbita**
- **Implementation model for creating secure Alexa skills with the Orbita platform**

Data "breaches" are unfortunately all too common and their repercussions are very serious and expensive – first, for the patients whose privacy has been compromised, but also for the responsible healthcare organization who must answer to (and pay fines to) the government bodies who set and enforce the regulations for healthcare data privacy and security. In the U.S., these regulations for healthcare are described by a regulation called HIPAA.

The goal of this white paper is to help explain basic HIPAA compliance to those with an interest in secure voice assistants for healthcare. We will summarize the key components for HIPAA compliance and, along the way, reference supporting systems, agreements, policies, frameworks, and methods that Orbita uses to help its customer and partners comply with HIPAA. We'll also describe general best practices for creating secure voice applications with Orbita that go beyond the requirements of HIPAA; and conclude with a general implementation model for creating secure Alexa skills using the Orbita platform.

WHAT IS HIPAA?

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and its subsequent extensions and modifications, are a set of U.S. regulations designed to protect patient medical records and Protected Health Information handled by health insurance providers, health care providers, doctors, and hospitals ("Covered Entities") or their third-party service providers ("Business Associates"). HIPAA is administered and regulated by the U.S. Department of Health and Human Services Office for Civil Rights ("OCR").

Protected Health Information ("PHI") is any healthcare information, including medical diagnoses, lab reports, vital data measurements, drug prescriptions, and more, that can be identified to an individual by what HIPAA refers to as Identifiers.

While the overall HIPAA regulations cover a broad set of requirements, those that pertain to voice applications are generally contained in two HIPAA rules: the Privacy Rule and the Security Rule.

What is the HIPAA Privacy Rule?

The HIPAA Privacy Rule ("Privacy Rule") includes regulations to limit the use and disclosure of PHI in healthcare treatment, payment transactions, and operations by covered entities. The Privacy Rule was established as the first United States national standard for protecting patients' personal or protected health information ("PHI"). It seeks to protect the privacy of patients by requiring doctors to provide patients with an account of each entity to which health care providers disclose PHI for administrative purposes, while still allowing relevant health information to be used within the proper context and authorized channels.

Specific safeguards are required to be in place that protect the privacy of PHI and set limits and conditions regarding the use and disclosures allowed without patient authorization. The Privacy Rule also gives patients the right to access their health information, including the rights to request copies, review, and update their PHI.

The Privacy Rule applies to all PHI including physical media and records, as well as electronic PHI or "ePHI."

Identifiers that may classify information as PHI include:[1]

- **Names**
- **Dates, except year**
- **Telephone numbers**
- **Geographic data**
- **FAX numbers**
- **Social Security numbers**
- **Email addresses**
- **Medical record numbers**
- **Account numbers**
- **Health plan beneficiary numbers**
- **Certificate/license numbers**
- **Vehicle identifiers and serial numbers including license plates**
- **Web URLs**
- **Device identifiers and serial numbers**
- **Internet protocol addresses**
- **Full face photos and comparable images**
- **Biometric identifiers (i.e. retinal scan, fingerprints, voice prints)**
- **Any unique identifying number or code**

What is the HIPAA Security Rule?

The HIPAA Security Rule establishes national standards to protect ePHI created, received, processed, or maintained by, or on behalf of a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

These safeguards are based on the Security Rule requirements, risk assessments, and application of industry standard security controls. HIPAA also requires that a Business Associates Agreement ("BAA") be in place with any third-party suppliers that handle or may handle ePHI, ensuring that proper review and requirements are extended to address any associated risks.

The Privacy Rule was established as the first United States national standard for protecting patients' personal or protected health information ("PHI").

The State of HIPAA Among Voice Platform Vendors

In April of 2019 Amazon announced that a version of their virtual assistant technology, Alexa, is now HIPAA-eligible. This means that it's available for applications that are subject to the data privacy and security requirements of HIPAA and that Amazon is willing to consider executing a BAA with Alexa skill developers who want to create HIPAA-compliant skills. As of this writing (August 2019), the new HIPAA-eligible version of Alexa is available to a limited number of developers by invitation only from Amazon.

Google has not made any claims of HIPAA-compliance for their Google Assistant voice platform but does offer other HIPAA-eligible cloud services that can be used for creating voice-powered virtual assistants that operate outside the Google Assistant framework.

In April of 2019 Amazon announced that a version of their virtual assistant technology, Alexa, is now HIPAA-eligible.

Orbita qualifies as a Business Associate in the HIPAA parlance.

HIPAA-Compliant Voice Applications with Orbita

While both Amazon and Google have shown their intentions to support HIPAA, full compliance is an activity of understanding and adhering to the regulation across all aspects of the business. Orbita provides software and services to healthcare organizations for designing, building, and maintaining virtual assistants that can be deployed to voice assistant platforms like Amazon Alexa and Google Assistant, web and mobile chatbots, and other conversational user interfaces. Orbita qualifies as a Business Associate in the HIPAA parlance.

Whether you are seeking a voice solution for clinical trials, call center operations, remote patient monitoring, in-facility operations, or a unique customer service in the healthcare space, you are likely concerned with ensuring compliance with HIPAA. Orbita's HIPAA strategy includes a cloud-based platform built from the ground up with data privacy and security safeguards in place to ensure HIPAA compliance. As a business, Orbita also maintains the organizational roles, policies, procedures and infrastructure to comply with the latest HIPAA rules.

Administrative Safeguards

The HIPAA Administrative Safeguards establish the administrative processes and procedures for an organization's HIPAA program. These safeguards are further broken down into standards including:

- Security management processes
- Assigned security responsibility
- Workforce security
- Information access management

- Security awareness and training
- Security incident procedures
- Contingency planning
- Evaluation
- Business associate contracts and other arrangements

Orbita's HIPAA strategy includes a cloud-based platform built from the ground up with data privacy and security safeguards in place to ensure HIPAA compliance.

Orbita has an established information security management program (ISMP) that addresses the administrative safeguards required of a business associate. With the understanding that security risks continue to change, Orbita has ongoing risk assessments and monitoring activities to ensure that all controls are effective and meeting objectives.

HIPAA's Adminstrative Safeguards require a BAA to be in place with third-party suppliers appropriate to their access, handling, or use of ePHI. Assurances are needed from them to ensure that they understand HIPAA and how they can negatively impact plans for safeguarding ePHI.

Orbita will execute a BAA with clients if required. Orbita also reviews all its suppliers and vendors to determine their access and risks to protection of ePHI. Pending each supplier review, appropriate agreements are executed, including a BAA when applicable.

Physical Safeguards

The HIPAA Security Rule requires that business associates and covered entities have physical safeguards and controls in place to protect ePHI.

The HIPAA Security Rule requires that business associates and covered entities have physical safeguards and controls in place to protect electronic Protected Health Information (ePHI).

These safeguards provide a set of rules and guidelines that focus on the physical access to ePHI through facilities, equipment, and other durable resources.

Orbita has physical security controls in place to ensure protection against threats that could affect electronic health information under Orbita's control. Relevant training is required for all new hires and for all employees when changes are made to any systems or processes that would affect the effectiveness or performance of such controls - or when new risks are introduced.

Technical Safeguards

Technical safeguards apply to the systems, operations, and staff required to ensure protection of ePHI. They include:

Access Control

Access control as it relates to the Security Rule, needs to determine the access control capability of all information systems handling ePHI and ensure that system activity can be traced to a specific user. Access controls may include policies, procedures, and processes to support what access needs to be granted, controlled, and monitored. Equally important is the control of access to update the policies, procedures, and process documentation to ensure that integrity is maintained by authorized individuals.

Orbita has policies and procedures in place for access control and monitoring to support user identification and tracking.

Orbita's systems are setup and configured with active vulnerability monitoring and response systems to protect for all data operations.

Audit Controls

Audit controls must be in place for hardware, software, services, and procedures that record and examine activity in information systems containing or using ePHI.

Orbita's ISMP has established internal audit procedures to review and monitor the assets, information, data, and user activities associated with ePHI. Orbita's systems are set up and configured with active vulnerability monitoring and response systems to protect for all data operations. Orbita uses Amazon AWS services including, but not limited to Amazon CloudWatch, Amazon Inspector, and Amazon Guard Duty. Alerts, warnings, and events are constantly reviewed and as required, responded to by Orbita's 24x7x365 operations team to investigate and address any issues that arise.

Integrity

Protecting the integrity of ePHI is a primary goal of the Security Rule. The Integrity standard requires a covered entity to: "Implement policies and procedures to protect electronic protected health information from improper alteration or destruction."

Orbita qualifies as a Business Associate in the HIPAA parlance.

Orbita's platform is hosted on Amazon AWS with which Orbita maintains a BAA. A secure container model is used with separate Virtual Privacy Clouds and Security Zones. Each Orbita deployment includes development, staging, and production configurations that are separated to restrict access and further protect ePHI. Finally, all data in the Orbita system is fully encrypted both at rest and in transit using AES-256, TLS, and HTTPS.

Person or Entity Authentication

This HIPAA standard requires that you validate a person's identity to confirm they are who they say they are.

Orbita's standard configuration employs a multifactor authentication approach to ensure that the person is authenticated based on a combination of two or more factors including a one-time authentication with a passcode, token, and/or a pin code.

Voice applications over smart speakers and other voice-enabled devices require special approaches to authentication. One approach is to assign a user to a specific device on the assumption that the device is only physically accessible to that user. Users created within the Orbita system can be set up and assigned to a specific voice assistant device. Orbita supports voice-based authentication requiring a user to verbally speak a personal identification number (PIN) or passphrase. Orbita also supports multi-factor authentication wherein the user enters a PIN or passphrase that triggers a separate temporary PIN sent via a text message, in-app message, or email message for a secondary confirmation.

Voice applications over smart speakers and other voice-enabled devices require special approaches to authentication.

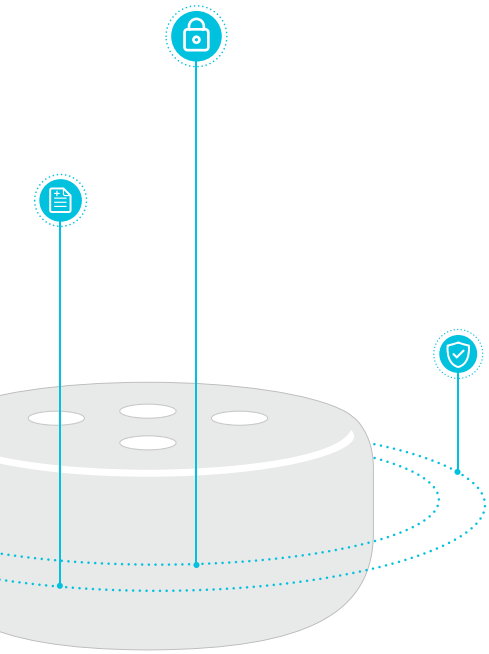
Transmission Security

Covered entities are required to have effective protection of ePHI data-in-motion (data being transmitted) electronically. Encryption must be used when ePHI is transmitted electronically..

Orbita has a supporting Cryptography policy that addresses data being stored and transmitted. Tenets of the policy include:

- Protection from ePHI being altered without detection
- Encrypted as appropriate and applicable
- ePHI shall be rendered unusable if intercepted by unauthorized individuals
- Encryption used for data at rest and data transmission
- Use of symmetric and asymmetric keys where applicable
- Use of non-proprietary, common FIPS-based supported cryptographic algorithms
- No decryption tools stored in same area as encryption tools

All traffic between services in Orbita is encrypted using TLS 1.2 or greater. Web-based services, including interfaces for all end user web-based applications are secure using HTTPS to protect the transmission of data.



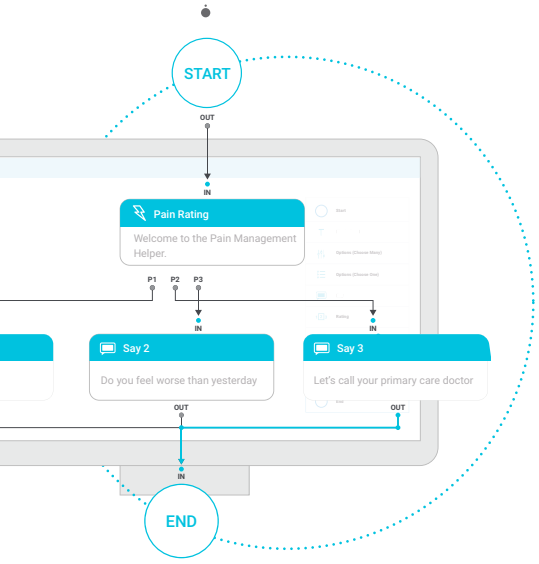
BEST PRACTICES FOR SECURE VOICE ASSISTANTS BEYOND HIPAA

While Orbita provides a HIPAA compliant platform, solutions built with Orbita still need to be thoughtfully designed and implemented to ensure both compliance and general security. It's possible for developers using the Orbita platform to implement sub-optimal solutions that expose PHI in a way that may be neither secure nor compliant.

Developers using the Orbita platform should follow the best practices listed in this section for creating secure voice assistants.

Anonymized User Accounts

Orbita recommends leveraging Orbita's anonymous accounts for users created and managed within the secure Orbita environment. With this approach, only a unique token is passed from Orbita to the voice assistant (e.g. Amazon Alexa) and no identifying user account information or PHI is shared with the voice service. Please see the next section ("Architecting Secure Voice Apps with Orbita using Alexa") for more detail on this approach.



Limit or Disable Voice Cards

Orbita allows for posting content to voice "cards" that are displayed within the voice service account. For example, content can be written to the Amazon Alexa voice cards visible using the alexa.amazon.com portal or the Alexa mobile app. It is important to limit the information written to these cards or to use only anonymous accounts.

Limit or Disable Voice Analytics

Like voice cards, it may be necessary to disable and or limit the patient specific information sent to the analytics and reporting services. Orbita provides the feature to disable the analytics down to a specific voice intent.

Limiting PHI

Perhaps the most obvious and surest way to deliver patient privacy and data security is to eliminate the transmission of PHI in voice assistant applications altogether. Depending on the business need, very powerful and valuable voice applications for healthcare are possible that do not require PHI. For many healthcare organizations, this may be the best first step into the brave new world of smart voice assistants.

Account Linking Using a Secure Provider

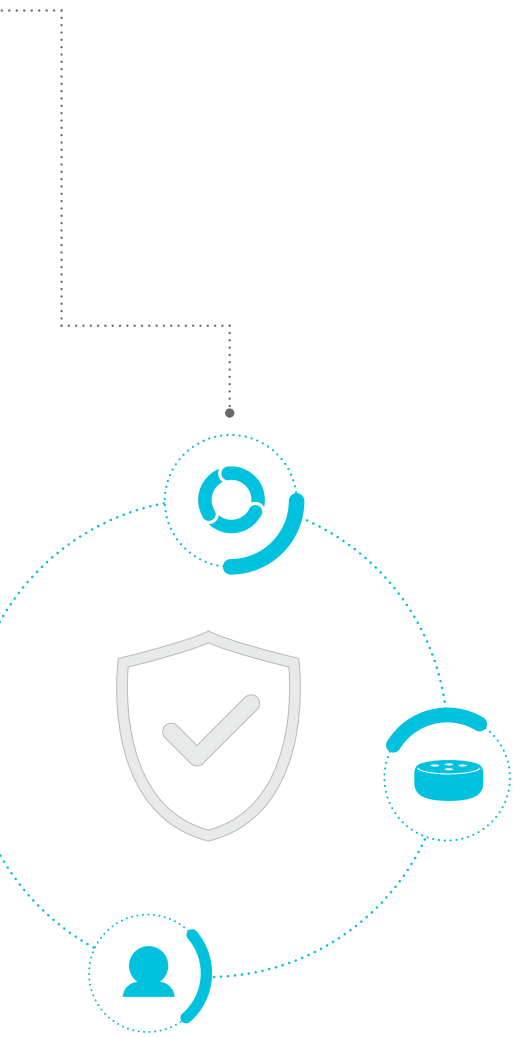
Orbita supports and suggests the use of dedicated secure third-party authentication providers to perform the account linking required. Account linking lets you securely grant voice applications powered by Amazon Alexa, Google Assistant, and others to securely access data managed in another system. Orbita supports account linking to any third-party system that supports the Auth Code Grant Flow of OAuth 2, for example, Facebook or Google, as well as Orbita's own OAuth service.

Application developers and user interface designers should consider the modalities available (voice, chat, touch screens, buttons, etc.) and the data that may be exchanged over these interfaces.

Other Guidelines

While voice technology might be secure from the standpoint of how data is protected once it is heard by the voice assistant, there are factors to consider that are outside the control of the technology itself. For example, only common sense can prevent someone from speaking sensitive information to a voice device in a crowded room. Application developers and user interface designers should consider the modalities available (voice, chat, touch screens, buttons, etc.) and the data that may be exchanged over these interfaces.

It is also important to consider the options that make the best sense for the type of information being collected, including the situation or context the person might be in. As a best practice, a form of a warning or notice provided at the start of the conversation or within the dialog can be used to prevent the user from sharing sensitive information.



ARCHITECTING SECURE VOICE APPS WITH ORBITA USING ALEXA

This section describes Orbita's approach to Securing Alexa Voice Skills in a way that ensures:

- Amazon has no ability to correlate an Amazon account with an Orbita account
- Amazon has no access and authorization to PII/PHI securely stored within Orbita Cloud

Consider this use case. John Smith is an individual using an Amazon Echo at home to monitor and improve adherence to an experimental prescription drug he's taking as part of a clinical drug trial. The Amazon Echo device allows him to indicate when he's taken medication *(e.g. Alexa, I've taken my 9 AM medication)* as well as hear a report on his overall medication adherence.

Even though John Smith is using an Amazon Echo to provide information to Orbita, Amazon has neither the ability to correlate a relationship between John Smith, Amazon, and Orbita; nor the ability to access any of John Smith's PHI/PII stored securely within Orbita.

The data flow diagram outlined in **Figure 1** describes the process used by Orbita to securely authenticate John, link accounts between Alexa and Orbita, and securely transmit data for processing.

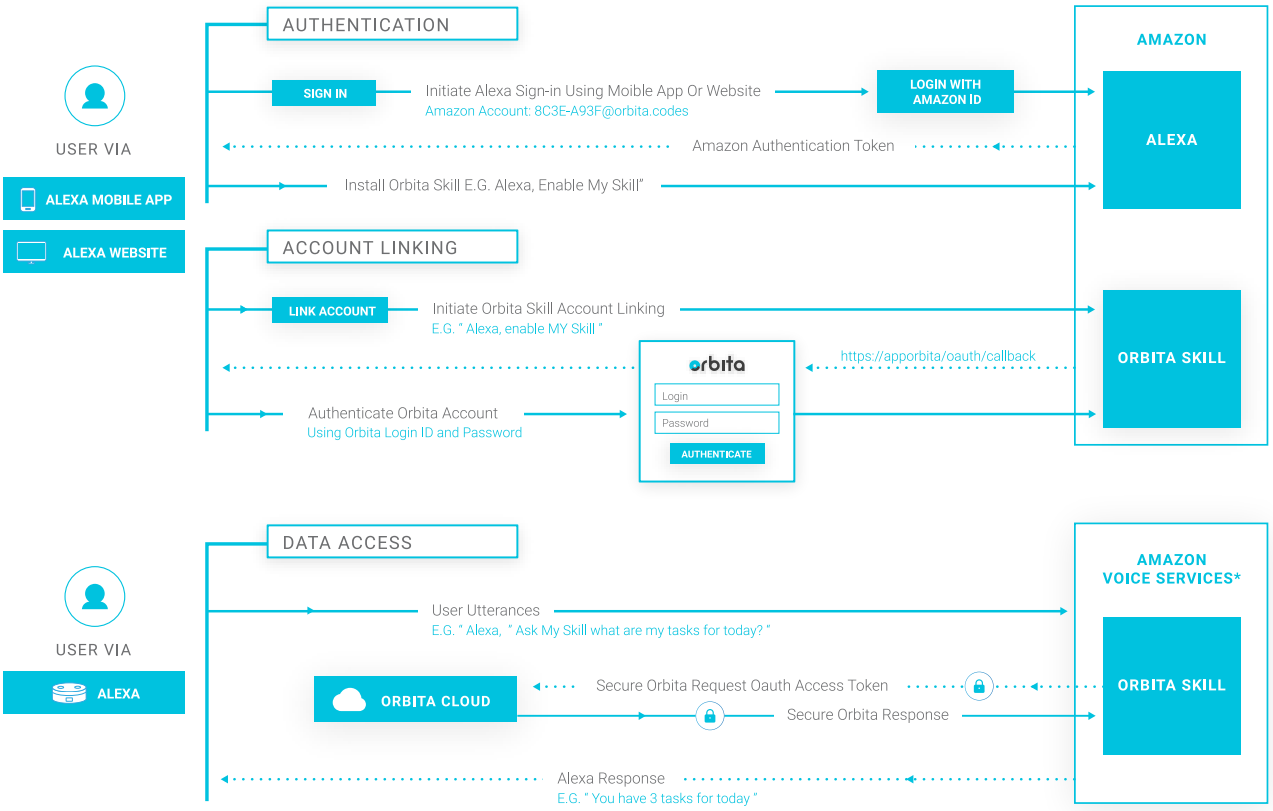


Figure 1: Orbita's Approach to Securing Alexa Voice Skills

Account Linking

Once the user has access to the Amazon Alexa account, the user enables the Orbita Voice Skill using the Alexa Companion App and links the Orbita Voice Skill to their Orbita account **(see Figure 2).** Doing so provides the Orbita Voice Skill with the authorization needed to access information securely from the Orbita Cloud.

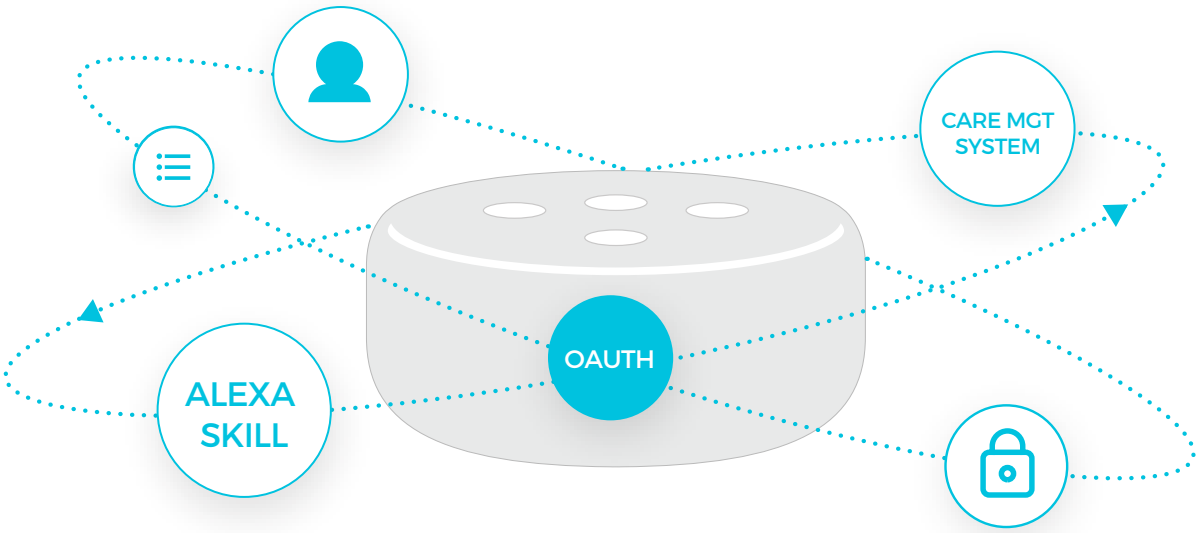


Figure 2. Alexa Skill and Account Linking

From within the Amazon Alexa mobile app (or web app), a user searches for and enables the Orbita Voice Skill. Once enabled, the Orbita Voice Skill displays in the list of available skills for that user's account.

Upon initiating the "account linking" process, the user is presented with a username/password challenge. Once the user successfully provides their Orbita credentials, Orbita generates a *user authentication token*. This token is used by the Orbita Voice Skill to prove that it has been granted permission to access the information on behalf of the user.

Note: Orbita uses the OAuth v2 protocol to establish the link between Orbita and the Orbita Voice Skill.

From the Voice Assistant, the Orbita Skill receives a Voice Request, which is a packet of information that includes:

- The Intent that matched the user's request E.g. GetMedications
- Any slot values
- And various metadata values, including time of day, session ID, etc.

The Orbita Skill uses the information to determine how to satisfy the request. In this example (Intent) the Orbita Skill would securely retrieve a list of the user's medication from the Orbita Cloud, using the user authentication token established during Account Linking, and assemble the appropriate response. The Orbita Skill returns its response to the voice assistant in the form of a Directive which includes the specific instructions for the Amazon Echo.

The Amazon Echo receives the *Directive* and delivers the voice experience to the user.

ABOUT ORBITA, INC.

Orbita provides conversational AI technologies and services for healthcare organizations to create secure, enterprise-grade voice and chatbot-powered virtual assistants. Orbita's HIPAA-compliant platform powers solutions that increase operational efficiencies and improve consumer, patient and member experiences to enhance remote patient monitoring, population health, customer service, member wellness, clinical trials and more. Leading digital health innovators rely on Orbita including Amgen, American Red Cross, Brigham and Women's, Deloitte, Mayo Clinic, and Pillo Health. **www.orbita.ai**

If you're considering a secure, voice-powered virtual assistant for your healthcare organization, contact Orbita. We are the healthcare leader in conversational AI for enterprise voice and chatbot-powered virtual assistants and can help you navigate these new waters.

Click here to request a complimentary HIPAA-compliant conversational AI consultation with Orbita.

REQUEST CONSULT

During this session, an Orbita voice security expert will help you understand the implications of HIPAA for voice solutions in your organization and help you identify opportunities to tap the potential of transformative, secure voice-first applications.

References

- www.xda-developers.com/microsoft-survey-voice-assistant-privacy-concern/ • HIPAA - https://www.hhs.gov/hipaa/ • Amazon HIPAA-Compliance - https://aws.amazon.com/compliance/hipaa-compliance/
- Business Associates Agreements - https://www.hhs.gov/hipaa/for-profe ssionals/covered-entities/ sample-business-associate-agreement-provisions/ • De-identification of PHI - https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/
- U.S. Department of Health and Human Services Training Guidelines - https://www.hhs.gov/sites/default/files/fy18-cybersecurityawarenesstraining.pdf