AMAZON HALO PRIVACY 101

Amazon Halo combines innovations in artificial intelligence and computer vision with medical science to help customers improve their health. With Halo, customers can trust that their Halo health data is protected and in their control. Customers can easily manage and download their Halo health data, delete it, or limit access to it if they share an Amazon account with household members. We've built strict protection mechanisms for customers' most sensitive Halo health data, like images captured when a customer uses Body, speech samples captured when a customer uses Tone, and Movement Health assessment videos. This sensitive data is stored locally in the Halo app on the customer's phone by default, when possible, and is automatically deleted after it's processed. In doing so, we ensure that no one ever hears Tone speech samples, Movement Health assessment videos are not accessed, and body scan images are only viewed by the customer—we do not use any of the three datasets for improving our machine learning algorithms.

We have created secure databases to store customers' Halo health data within Amazon. All personally identifiable data within those datasets are hashed to protect the customer's identity and the datasets are strictly access-restricted at Amazon and never sold to any third parties. Customers can link their Halo health data to a third-party program if they choose, and can cancel that link at any time from the Halo app settings to end data sharing. By never compromising on customer privacy, we continue to earn our customers' trust every day. Learn more about Amazon Halo at www.Amazon.com/HaloBand.

Halo health data includes data like activity and sleep scores, movement scores, step count, heart rate, body fat percentage, demographic information. Halo health data is stored in the secure Amazon cloud and is encrypted in transit and at rest in the cloud. Customers can download or delete their Halo health data any time directly from the Halo app. We do not use Halo health data for marketing, product recommendations, or advertising. We do not sell customers' Halo health data. Customers' Halo health data is strictly access-restricted at Amazon.

Customer requests to Alexa are not treated as Halo health data, but customers can review and delete their voice recordings at any time from their Alexa voice history.

PRIVACY CONTROLS

Amazon Halo customers place considerable trust in us just by using our services. We take this responsibility seriously and have built tools that make it easy for customers to protect and control their Halo health data.

Profile Protection: We know that customers may share their Amazon account with household members, but that doesn't mean that customers always want those people to be able to view or access their Halo health data. To ensure that Halo health data is personalized and distinguished from others in the household, we require customers to create or choose a unique profile when they first use Halo. After selecting their profile, customers are prompted to add claim credentials to their profile (a mobile phone number or email address) that are verified via a one-time passcode. This occurs by default when customers set up their profile in Halo and provides customers with a safeguard for their Halo health data. After adding claim credentials to their profile, customers are prompted to validate a one-time passcode on any subsequent login to the Halo app. Halo automatically prompts customers who choose to bypass claim credential entry with in-app reminders to enter and validate their claim credentials and protect their profile. These reminders are pinned to both the Halo app home screen and the Halo app settings screen until the customer either adds claim credentials to protect their profile or explicitly dismisses the reminders.

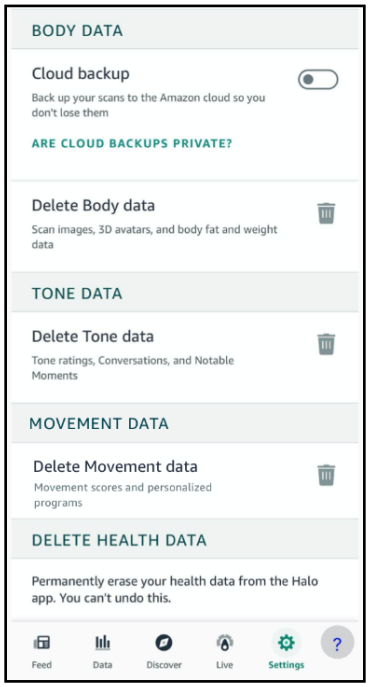
Customers who are not in physical possession of their smartphone can sign out of their Halo account remotely by deregistering the Halo app from Manage Your Content and Devices on Amazon.com. This prevents anyone else who may have access to their smartphone from viewing their Halo health data.

Connect Alexa with Halo: The Halo Band microphone is used exclusively for Tone and is not integrated with Alexa. While customers can't make an Alexa request directly from their Halo Band, they can choose to enable the Connect Alexa to Halo setting so they can access their Halo health data by simply asking their Alexa enabled devices. Once enabled, customers can ask, "Alexa, how did I sleep last night?" or "Alexa, how much activity have I had today?" and Alexa will answer with their Halo data. While customers can always ask Alexa for their Tone results – like "Alexa, how did I sound today?" – the Alexa-enabled device's microphone cannot be used to record or analyze their Tone. Tone analysis can only be done from the Halo Band and Halo app.

SETTING UP YOUR PROFILE PIN
From the Amazon Alexa app:
Step 1: Use an existing voice profile or create a new voice profile from the profile settings in the Alexa app
Step 2: Create a PIN for the voice profile from the profile settings in the Alexa app
From the Amazon Halo app:
Step 3: Enable PIN protection for Halo health data from the Alexa settings in the Halo app.

Customers who share Alexa-enabled devices can add an additional layer of security to their Halo health data by choosing to require a profile PIN. Once enabled, customers must verbally enter the PIN before Alexa will respond with their Halo health data. Halo customers can enable a 5-minute timer on their PIN from the Halo app settings if they don't want to enter the PIN with every voice request. Once enabled, Alexa will not require customers to re-enter their PIN for any subsequent Halo health data questions for five minutes.

Halo Health Data Download and Deletion: Customers can download all the Halo health data associated with their profile and review it on their own terms. After opening the Halo app, it takes just a few taps for customers to download their data. A link to download the data is delivered to the claim credential that the customer previously used to verify and protect their profile. The link to their raw Halo health data automatically expires after seven days.



Similarly to downloading data, customers can delete all Halo health data associated with their profile from the Halo settings. Deleting this data is a permanent action and it cannot be recovered after it's been deleted. However, if a customer decides they want to stop using Halo and leave no Halo health data behind or if they simply want to reset their data and start from scratch, this control allows them to make that choice. Once a customer deletes their data in the Halo app, they're automatically logged out of the app and cannot log back in with their profile until all of the Halo health data associated with the profile has been deleted.

Delete all Tone, Body, and Movement Health Data: Customers can also delete all of their retained Body, Tone, and/or Movement Health data. Body data deletion includes historical data on their body fat percentage, scan images, and associated scan image assets (i.e., 3D body model and texture maps generated from the scan which are used to personalize the 3D body model). Tone data deletion includes voice profile, Tone analysis results, and any speech samples currently stored on the customer's smartphone. Movement Health data deletion includes all scores generated from movement assessments and personalized movement programs.

PROTECTING BODY DATA

The Amazon Halo Body feature allows customers to obtain an accurate body fat percentage measurement from the comfort and privacy of their own home. To get their body fat percentage, customers take a body scan that generates four images—front, back, and both sides. Along with obtaining body fat percentage results and their scan images, customers receive a personalized 3D body model so they can see a representation of how their body looks at the time of that scan and then use the 3D body model to track changes over time. From the Body page, customers can hide their scan images and body fat results so they don't have to worry about a curious friend looking over their shoulder and seeing their scan photographs or body fat percentage.

Body scan images are processed in the secure Amazon cloud. They are encrypted in transit and processed within seconds, after which they are automatically deleted from Amazon's systems and databases. All scan images are fully deleted within 12 hours. The scan images are not viewed by anyone at Amazon and are not used for machine learning optimizations. The scan images and all associated scan assets are stored exclusively in the Halo app's local storage on the customer's smartphone—the scan assets are never shared with any other app, including the smartphone's default photo gallery, unless the customer explicitly exports the images. No one but the customer ever sees the scan images unless the customer chooses to share them.

Storing body scan images in the Halo app's local storage means that the scan images and assets are permanently deleted when the app is uninstalled and cannot be accessed if the customer logs in on a new smartphone. Customers can choose to opt in to cloud backup for their scan images to ensure they can recover their images if they change phones. Nobody at Amazon accesses these images. Scan images and scan assets stored in the cloud are secured using Amazon data protection best practices, including encryption and the use of least-privilege access principles, which block Amazon personnel from accessing the encrypted data. Customers can always opt out of cloud backup later via the Halo app settings, even if they've previously opted in. As soon as they opt out, their images are deleted from the cloud, but continue to be stored in the Halo app's local storage on their smartphone. Scan assets stored in the cloud are protected with controls required for the most sensitive classes of stored data at Amazon.

PROTECTING TONE DATA

With Tone, customers can use the microphones built into the Amazon Halo Band or the Halo app to understand how they may be perceived by others based on their tone of voice.

Customers must opt in to Tone if they want to use it and can do so by setting up a Halo voice profile. The Halo voice profile is based on technology that identifies when the customer is speaking—this technology trains Tone to only analyze the speech samples of the customer who enabled it. The more the customer uses Tone, the better Tone gets at recognizing their unique voice profile. The microphones in the band are off until and unless customers have opted in to Tone by setting up a voice profile. Customers who have enabled Tone can then turn off the microphones on the band by holding down the button on the band for three seconds, until the LED light flashes red. When the microphones are off, they are unable to collect speech samples for analysis.

Tone speech samples are transferred from the band to the Halo app over Bluetooth. To ensure no other apps on the customer's smartphone can see this data, it is encrypted with a key shared between the band and the Halo app. This key is exchanged at the time the band is paired with Halo, and a new key is generated and renegotiated each time the band is deregistered and then registered again with Halo (for example, when a Halo Band is resold or paired with a different smartphone). The encryption algorithm used is AES-256 with GCM. All data transferred between the band and the Halo app is encrypted using this key.

All speech samples collected for Tone are processed locally on the customer's smartphone. Samples used to assess Tone are never sent to the cloud. No one—including the customer—ever hears them. By storing and processing speech samples locally, the data is always within the customer's control. Speech samples are automatically deleted after processing and are never used to train machine learning models.

A **Tone voice profile** is an acoustic model of a customer's voice characteristics. Tone is an opt-in feature that requires that a customer set up a voice profile to use it by reading aloud and recording a series of statements provided to the customer in the Halo app. The voice profile trains Tone to analyze only the customer's voice.

Tone speech samples are temporary recordings of speech. Once it's set up, Tone processes speech samples. Then it analyzes how a customer may be perceived by others and displays a summary of the analysis in the Halo app.

Following processing, Tone analysis results are stored in the secure Amazon cloud so that customers can continue to access their results even if they get a new smartphone. Tone analysis is essentially a summary of the Positivity and Energy of a given phrase. It never includes raw audio data or audio transcriptions. We do not apply machine learning to the Tone analysis results of individual customers to optimize our Tone algorithm. Tone analysis is treated as Halo health data and customer identifiers associated with the tone analysis data are one-way hashed with a secret key so that it cannot be traced back to the customer associated with it (see Data Handling for more on how we protect Halo health data).

PROTECTING MOVEMENT DATA

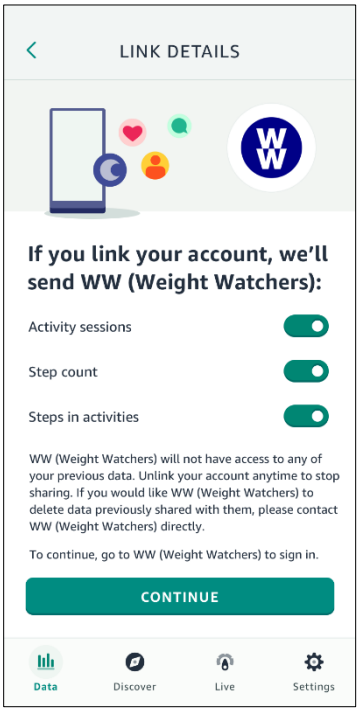
The Movement Health feature allows customers to analyze and improve their mobility, stability, and posture through personalized exercise programs. The experience begins with a short video assessment where customers complete several movements (e.g., forward lunge, squat) that are analyzed by Halo using their smartphones' camera. After completing the assessment, customers receive a movement score (0-100 scale), sub-scores for mobility, stability, posture, and a personalized exercise program.

Movement Health assessment videos are processed in the secure Amazon cloud. They are encrypted in transit and processed within seconds, after which they are automatically deleted from Amazon's systems and databases. Before deletion, Amazon's computer vision technology identifies areas of movement restriction from the video. With that data, we're able to determine movement scores and recommend exercises targeted to a customer's movement needs. All assessment videos are fully deleted within 12 hours. The assessment videos are not viewed by anyone at Amazon and are not used for machine learning optimizations. The assessment videos are not retained in the Halo app's local storage which means no one can access them from a customer's smartphone.

DATA HANDLING

Storing and Usage of Customer Halo Health Data: Halo health data is not used for marketing, product recommendations, or advertising. All customer identifiers are one-way hashed with a secret key to ensure there is no way to map stored Halo health data back to the customer who recorded it. This means that none of the Halo health data collected can be tied back to a customer and the Halo health data cannot be combined with or correlated with any other data Amazon might store about that customer. This approach ensures that customers' Halo health data cannot be used as an input in recommending products elsewhere on Amazon including, but not limited to, Amazon.com, Alexa, and Prime Video. It also means that no employee of Amazon or anyone else with access to a customer's Halo health data can identify the customer associated with it.

All customer identifiers linked to a customer's Halo health data are protected using a one-way cryptographic hash function with a key stored in the AWS key management service that is only accessible by the service responsible for performing the hash. This is a one-way operation; Amazon identifiers like customer IDs can be converted to hashed IDs but it is impossible to convert a hashed ID back into a customer ID. We use distinct namespaces for each hashed data store (e.g., the same customer's data stored for display in Halo and for use in improving machine learning algorithms will have different hashed IDs) and we ensure the hashed IDs are never propagated outside of these data stores. These measures ensure additional data that could potentially identify the user can never be associated with the hashed IDs.



Halo health data is not stored as part of Alexa voice recording responses and is not reviewable in customer's Alexa voice history. However, customer requests to Alexa are not treated as Halo health data and customers can review and delete their Alexa voice recordings at any time from their Alexa voice history in the Alexa App or in their Alexa Privacy Settings online. To learn more about the features that give customers control and transparency over their Alexa experience, visit the Alexa Privacy Hub.

Sharing Data with Third Parties

Account linking: Customers can choose to link their Amazon Halo account to other third-party programs to obtain even more benefits. For example, customers who link their Halo account with their WW (formerly Weight Watchers) account can earn FitPoints based on their Halo activity score. Account linking is always opt-in. We give customers a bulleted, plain English list of the data they are consenting to share and surface the third party's privacy policy in case the customer would like to review it again. Customers can opt out of account linking any time from the Halo app settings. We only allow third parties to request data from customers that is useful in providing a service or feature to customers and limit, through the terms of our contracts, the use of the data they do request.

Sharing Data with Content Providers: Some of the content offered in Discover is created by third-party content providers. No personally identifiable data is shared with these content providers without the customer's agreement. For example, content providers—like Headspace—only receive aggregated, anonymized data about

their programs. This aggregated and anonymized data can help them improve the experience they provide Halo members, like data which informs them which of their programs is most popular among customers or which programs have the highest completion rate.

BLE broadcasting: Customers can also connect to third party devices via Bluetooth Low Energy (BLE) and choose to broadcast their heart rate to the third party device. For example, with BLE broadcasting enabled, a customer completing a workout on a BLE-enabled treadmill would be able to see the heart rate from their Halo band on the treadmill's screen. No personally identifiable data is shared with the third party device when broadcasting data. To protect customer privacy, Halo encrypts broadcasted data in transit and allows BLE to connect to only one device at a time.

In summary, privacy and security are foundational to the way we designed Amazon Halo. Learn more about Halo at www.Amazon.com/HaloBand.