Starkey
Hearing Technologies

6600 Washington Avenue S.
Eden Prairie, Minnesota 55344
T: 1.800.328.8602

www.starkey.com

November 16, 2020

Reference: Wireless Hearing Aid Data Security Statement

Dear Sir/Madam:

Starkey Hearing Technologies wireless hearing aids use one of three different frequency bands and transmission protocols depending on the product. All technologies provide security; however, each uses a different method for this purpose.

900sync Wireless Hearing Aids

Starkey Hearing Technologies wireless hearing aids that operate either in the 902 to 928 MHz band or 863 to 865 MHz band use our 900sync technology. This technology utilizes a proprietary transmission method not based on any published standard. The processing within Starkey Hearing Technologies 900sync wireless hearing aids also uses proprietary digital modulation that incorporates a data whitener based on a complex polynomial to scramble the data. These two design approaches prevent other commercially available devices from readily discovering, intercepting, interpreting, or injecting transmitted data, and effectively ensure security of transmitted data. In addition, the low output power and antenna size limit the range at which Starkey Hearing Technologies 900sync wireless hearing aid transmissions can be readily received to approximately 15 meters. This provides a pragmatic limit to the ability to intercept data transmitted wirelessly.

The reverse is also true. The Starkey Hearing Technologies 900sync wireless hearing aid family is unable to transmit or receive data in any transmission protocol other than its own proprietary transmission protocol. That, combined with the very limited range to which it can transmit, effectively ensures that the Starkey Hearing Technologies 900sync wireless hearing aid family cannot discover, intercept, interpret, or inject transmitted data associated with other devices.

900sync hearing aids can receive audio information from the SurfLink Media, SurfLink Mobile, SurfLink Remote Microphone, and SurfLink Mini Mobile accessories using a Starkey proprietary encoding method. The ability to receive audio from SurfLink accessories can be disabled on the hearing aids. The range of these accessories is about 15 meters.

900 sync hearing aids can also receive audio information from the other hearing aid of a binaural pair during a telephone call. This audio streaming only occurs when enabled by a hearing aid button press to select a memory where this streaming is enabled or by a DC magnetic field near the hearing aid, such as that from a telephone handset, which enables streaming between the two hearing aids of the pair when the magnetic field is present.

900sync hearing aids can receive data commands from the SurfLink Remote and SurfLink Mobile using a Starkey proprietary encoding method. These commands are used to control the basic functionality of the hearing aids (change volume and memory settings). A SurfLink Remote or SurfLink Mobile must be paired to a specific set of hearing aids. The hearing aids can transmit data commands to each other, similar to the SurfLink Remote. These commands are used to change volume and memory settings.

When using the SurfLink Mobile or SurfLink Mini Mobile as a cell phone accessory, the hearing aid microphones can be used to transmit the patient's voice (JustTalk feature) during a phone call. The JustTalk feature can be disabled on the SurfLink Mobile.

The SurfLink Media, SurfLink Mobile, SurfLink Remote Microphone, and SurfLink Mini Mobile devices are the only Starkey accessory devices that can capture and wirelessly transmit audio that can be successfully decoded by the hearing aids.

The SurfLink Programmer can detect the presence of a specific 900sync hearing aid within its range (about 10 meters). The programmer could also change the programming of a 900 MHz hearing aid within its range. The risk of program alteration can be mitigated by setting a hearing aid lock code in Inspire when the hearing aid is initially programmed.

2.4 GHz Wireless Hearing Aids

Starkey Halo, Halo 2, Halo iQ, Livio, Livio AI, and Livio Edge AI hearing aids "2.4 GHz hearing aids" operate in the 2.4 to 2.4835 GHz band and use a number of methods to provide secure communications.

Bluetooth Security

2.4 GHz hearing aids communicate with the Starkey 2.4 GHz Programmer, and with Apple iOS™[1] devices, (including the iPhone®[2]) and Android™[3] mobile devices[4] that use the Thrive hearing control application using the Bluetooth®[5] Low Energy protocol. In addition, the Starkey Hearing Technologies Remote, Starkey Hearing Technologies TV, Remote Microphone+, Mini Remote Microphone, and Table Microphone communicate with Halo iQ[6], Livio, Livio AI, and Livio Edge AI hearing aids using the Bluetooth Low Energy protocol to pair with the hearing aids and generate the encryption key used for sending commands to the paired hearing aids. In today's world, because information is being transmitted, there are occasionally concerns about the security of the information that is being sent.

The Bluetooth Low Energy protocol used in the 2.4 GHz hearing aids is very secure. From a technically descriptive standpoint, that protocol is based on RFC 4493, which employs a cipher-based message authentication code (CMAC) that uses the advanced encryption standard (AES-128) as the block cipher function. In practical terms, this means that once two devices are paired with each other, all information passed between the devices is encrypted and therefore effectively undecipherable by any other device.

The lone security risk exists only during pairing. 2.4 GHz hearing aids use LE legacy pairing. This

[1] iOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used under license by Apple, Inc.

[2] iPhone is a registered trademark of Apple, Inc.

[3] Android is a trademark of Google, Inc.

[4] The specific Apple iOS and Android devices supported by the Thrive Hearing Control app can be found on the Starkey Hearing Technologies *Smartphone Compatibility* web page.

[5] Bluetooth is a registered trademark of the Bluetooth Special Interest Group

[6] The Starkey Hearing Technologies TV Remote Microphone+, Mini Remote Microphone, and Table Microphone only operate with Livio, Livio AI, and Livio Edge AI hearing aids.

is convenient for the patient but is vulnerable to eavesdropping or man in the middle attacks during pairing[7]. During pairing, the devices each generate encryption keys and exchange them with the other device. If keys are stolen, it is possible, but very difficult, to decipher information sent from one device to the other. The probability of this occurring is remote for three reasons. 1) The equipment needed to acquire the keys is very specialized and expensive, 2) the range of the transmission is limited to around 10 meters, and 3) Pairing is only required to be completed once. An attacker would need to be present with said specialized equipment and in range at this exact time to obtain the link keys. Subsequent connections thereafter will not have this vulnerability and will be confidential. Therefore, it is highly unlikely that anyone would have the equipment necessary and be in a position to steal the link key during pairing. However, if security is a concern, it is suggested that while performing pairing a person do this in the privacy of their own home or in another trusted place to ensure that your key is not stolen during this process.

It is not possible to eavesdrop on audio streamed between the paired iPhone or Android phone[8] and the 2.4 GHz hearing aid by attempting to connect an intruder’s Bluetooth device to the hearing aid, since the Bluetooth protocol used encrypts the audio stream on a per-link basis.

Note that audio is streamed from a paired iPhone or Android phone to a 2.4 GHz hearing aid. Audio is only streamed from the hearing aid to a paired iPhone or Android phone when the Personal Voice Assistant 2.0 feature[9] is used. This feature is triggered by a hearing aid user control actuation and the stream lasts for up to 10 seconds to do voice recognition. The audio is transported over an encrypted BLE link. If a user is concerned about security or privacy, they can disable this feature using the mobile app. Also, the user can configure the feature to use the local microphone on the phone rather than hearing aid microphone to capture the user’s voice.

If the user’s iPhone or Android phone is off, its Bluetooth radio is off, or it is out of range when the hearing aid is powered up, it is possible for an unwanted device to pair and thus connect to the hearing aid. Note that a 180 second pairable timeout applies to all Bluetooth devices. After 180 seconds OR after a paired iOS/Android device is connected, a hearing aid will only accept connections from BLE devices that are already paired. This is our primary mechanism for mitigating a denial of service attack. If the unwanted device is able to connect to the hearing aid, it can exercise the existing controls of the hearing aid and prevent the user’s own iPhone or Android phone from connecting to the hearing aid. This would be detected by the user since the hearing aid would no longer respond to the Thrive app on the user’s iPhone or Android phone.

Therefore, a useful test to verify that no other Bluetooth device other than the user’s iPhone or Android phone is connected to the 2.4 GHz hearing aid is for the user to attempt to connect their iPhone or Android phone with the Thrive app to their hearing aids after hearing aid power-up. If the connection attempt succeeds, no other Bluetooth device can connect to these hearing aids as long as the hearing aids remain powered up, the iPhone or Android phone and its

[7] Once pairing has occurred, then all future communications are encrypted.

[8] Audio streaming from Android phones is only supported by Livio, Livio AI, and Livio Edge AI hearing aids.

[9] This feature was introduced in February 2020 with the Sydney program.

Bluetooth radio remains on, and the iPhone or Android phone remains within range of the hearing aids.

The Starkey 2.4 GHz Wireless Programmer can detect the presence of a specific 2.4 GHz hearing aid within the hearing aid range (about 10 meters). The programmer could also change the programming of a 2.4 GHz hearing aid within its range (10 meters) that is not paired to a mobile phone. The risk of program alteration can be mitigated by setting a hearing aid lock code in Inspire when the hearing aid is initially programmed. If such a code is programmed, the code must be entered before Inspire can read the hearing aid or change any of its programmed settings. We also disable Undirected Connectable Mode on the hearing aid when connected to a programmer. This prohibits other BLE connections from being established with the hearing aids.

The Starkey Hearing Technologies Remote, Starkey Hearing Technologies TV, Remote Microphone+, Mini Remote Microphone, or Table Microphone can detect the presence of a specific Halo iQ, Livio, Livio AI, or Livio Edge AI hearing aid within the hearing aid range (about 10 meters). The accessory can pair to hearing aids under the following condition:

- Hearing aid is not connected to a mobile phone
- Hearing aid is in pairable mode (i.e. within 180 seconds after power-up)
- Hearing aid is within 1 meter of the accessory (we typically recommend 6 inches or less when pairing with the RSSI filter). [10]

The accessory can send commands to a paired hearing aid thereafter within its range (10 meters), regardless of whether a mobile phone is connected or not.

However, the commands can only act within the limits (for example, raising or lowering volume) that have been previously programmed into the hearing aid by a hearing care professional.

Audio Broadcast Mode Security

The Livio, Livio AI, or Livio Edge AI hearing aids connect with the Starkey Hearing Technologies TV streaming device, the Remote Microphone+, the Mini Remote Microphone, or Table Microphone by using the Bluetooth Low Energy protocol to associate the hearing aid(s) with the TV streamer, Remote Microphone+, Mini Remote Microphone, or Table Microphone. However, no secure encrypted information is exchanged during this process. Once an association is established, the TV streamer and/or Remote Microphone+ then communicates with the Livio, Livio AI, or Livio Edge AI hearing aid(s) using a proprietary audio broadcast mode in which the audio stream is not encrypted. Note that audio is only streamed from an associated TV streamer, Remote Microphone+, Mini Remote Microphone, or Table Microphone to a Livio, Livio AI, or Livio Edge AI hearing aid. No audio is ever streamed from the hearing aid to a TV streamer, Remote Microphone+, Mini Remote Microphone, or Table Microphone.

Note that although the link between the Starkey Hearing Technologies Remote Microphone+

[10] In addition, these accessories use an RSSI filter to limit the communication range during pairing. The accessories don't have a display for the user to select their device during pairing, so the RSSI filter provides some level of discrimination so the correct hearing aids are paired. The RSSI filter is not used when sending commands after the accessory is paired to the hearing aid(s).

and the Livio, Livio AI, or Livio Edge AI hearing aid is not encrypted, the Classic Bluetooth link between a mobile phone (or other Bluetooth device) and the Starkey Hearing Technologies Remote Microphone+ is encrypted as described above under Bluetooth Security.

NFMI Radio Security

In addition to using the 2.4 GHz radio band for communications for accessories and smartphones, some Livio, Livio AI, and Livio Edge AI hearing aids also use Near Field Magnetic Induction (NFMI) for ear-to-ear radio communications between the two hearing aids in a binaural pair.

The security of NFMI radio communications is based on the very short range of NFMI communications. The range of the NFMI radio used in the Livio, Livio AI, and Livio Edge AI hearing aids is less than 30 cm.

General Considerations

Security can be enhanced on all Starkey wireless hearing aids by programming a hearing aid lock code into the hearing aid with Inspire. If such a code is programmed, the code must be entered before Inspire can read the hearing aid or change any of its programmed settings.

Please note that Starkey Hearing Technologies cannot guarantee absolute security. As with most systems, a concerted reverse engineering effort may be able to compromise the security aspects of Starkey Hearing Technologies' wireless devices.

Should you have any questions, please feel free to contact the undersigned.

Sincerely,

William J. Mitchell, PE
Principal Regulatory Affairs Engineer
bill_mitchell@starkey.com