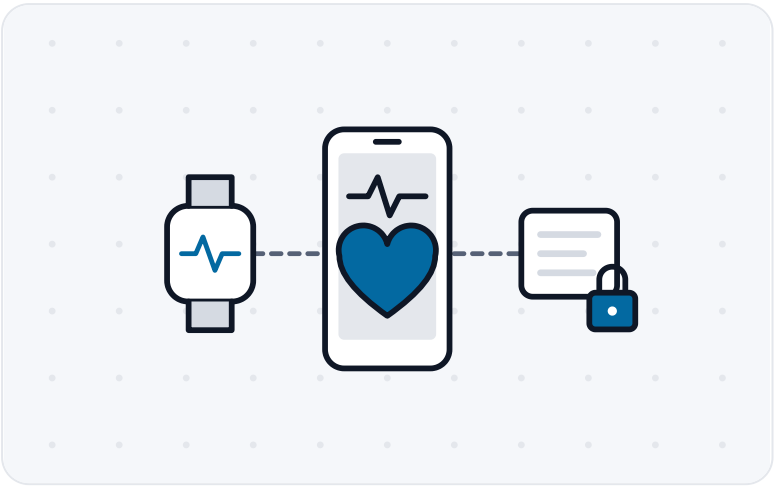
A-SIT Technology

E-Government Innovation Center

29 December 2023 Analysis · Mobile Security · Privacy & Crypto · 12 min read

Analysis of the Android Health Connect Programming Interface

Gerald Palfinger



Authors	Gerald Palfinger
Version	2023-12-27
Source	https://technology2.a-sit.at/en/publications/analysis-of-the-android-health-connect-programming-interface/
Note	Machine translation.

Key findings

- An app must declare and actively request the matching permission for every data category it reads through Health Connect.
- On first access, Health Connect asks the user; each category can be released individually for reading or writing.
- A newly installed app only sees data from the last 30 days, so that malicious apps cannot access all historical data.
- Health Connect requires a privacy policy, and access must be requested from Google before publication in the Play Store.

- Every access is logged; the accesses of the last 24 hours can be viewed in the settings.

A large amount of sensitive data is typically stored on smartphones. In combination with wearables and other smart diagnostic devices, smartphones also receive fitness and health data, which can provide detailed information about the user's health status. Modern smartphone operating systems offer a central interface for storing and retrieving these data so that they can be shared and analysed more easily. However, due to the abundance of personal data stored, data protection and security are of utmost importance. This report uses the example of the new Health Connect programming interface available on Android to show what steps are necessary for an application to access the centrally stored fitness and health data. It also shows what influence users have over access to their data and what security provisions are in place.

1. Introduction

With a variety of sensors, smartphones can record fitness data such as the number of steps taken each day. Dedicated fitness trackers and smartwatches, which are often worn on the body 24 hours a day as so-called wearables, are also becoming increasingly popular [1]. They can record a variety of information such as heart rate, oxygen saturation or respiratory rate, and use it to calculate relevant indicators such as calorie consumption or to detect sleep patterns, for example. Smart household appliances such as personal scales can also record further relevant information such as weight or muscle mass. These devices can be connected to the smartphone via interfaces such as Bluetooth Low Energy. The smartphone thus serves as the central storage for the collected data. However, manufacturer-specific applications are usually needed to read out the data. As a result, only the manufacturer's application, which retrieves the data from the device, usually had access to the respective data. Data from different devices could therefore usually only be analysed together if the devices came from the same manufacturer. To break up these data silos, smartphone manufacturers have developed interfaces that allow central storage and manufacturer-independent access to the data. Such centralised storage can make it easier to integrate different health and fitness applications, which allows better fitness and health profiles to be created. Given the abundance of stored information and the central access option, however, the question of data protection and security is of utmost importance. In particular, detailed access control that gives users the option of releasing individual fitness and health data would be desirable. This report examines how Health Connect is built on Android, in particular with regard to the privacy and security of the stored data. For this purpose, an application is used to read existing health data from an application and write it to the central Health Connect database. A separate application was also developed that reads the data out of the Health Connect system again. This report shows which prerequisites an application must meet in order to read the stored data, how the system manages the accesses, and what influence users have on the security of their fitness and health data.

2. Background

2.1. Health Connect

Both Android and iOS offer a central storage location for fitness and health data. While on iOS the HealthKit SDK introduced this as early as iOS 8 in 2014, Android has had one since 2022 with Health Connect. At first, this was a separate application that had to be installed via the Play Store. With the release of Android 14, however, Health Connect has become part of the system [2]. Before that, health and fitness applications could only exchange their data via application-specific interfaces such as Content Providers. With Health Connect, fitness and health data can now also be exchanged on Android via a standardised interface.

2.2. Related Work

In 2018, the fitness network Strava published a global heatmap with the anonymised route data that users had recorded with their smartphones and wearables. Despite the anonymisation of the data, sensitive conclusions could be drawn from the published heatmap. For example, the data made it possible to identify bases of military installations in crisis regions [3]. Individual persons stationed there could also be identified with the help of further data from the network. To protect sensitive locations, Strava therefore introduced a function for hiding them. With these so-called Endpoint Privacy Zones, a certain area around the sensitive locations is hidden in uploaded route recordings. However, [4] showed that this method offers hardly any protection. By using the coordinates where the route enters the Privacy Zone, the displayed distance of the activity, and road data, the effectiveness of the Privacy Zone can be reduced considerably. By combining the data, the sensitive location can even be determined in a large number of cases. In the evaluation of 1.4 million analysed activities, about 85% of the protected locations could be deanonymised.

There have also been data breaches at various online fitness services. In 2018, data of more than 150 million users of the fitness network MyFitnessPal was leaked [5]. In the same year, it became known that data from the fitness application PumpUp was accessible via an unprotected server [6]. This included highly sensitive data about the users: besides names and dates of birth, also health information entered by the users, such as alcohol and tobacco consumption, medications and injuries suffered. In 2020, it became known that more than 42 million records of the fitness company Kinomap were accessible on the internet without protection [7]. These included personal details such as names, country of origin and information about workouts completed. In 2021, over 61 million records from various wearables were leaked [8]. These included data from Fitbit and Apple's HealthKit. The data originally came from the service provider GetHealth, whose application can read out fitness and health data from various sources.

In [9], an attempt was made to find out which information users of fitness trackers share on social networks and how third parties can thereby form a picture of their identity. A tool was developed to answer this question. This tool models the information collected by the fitness trackers and released by the users on various social networks. In doing so, the tool shows which further personal information is released in an unwanted manner and which privacy risks this raises.

In [10], an attempt was made to determine users' habits when sharing information recorded by fitness trackers and other wearables. Potential concerns they have when sharing this information across a variety of platforms were also recorded. For this purpose, semi-structured interviews were conducted with a total of 30 participants. The evaluation of the results found that privacy and security usually play only a minor

role in the decision on whether potentially sensitive fitness data should be shared with others. As a rule, the decision on whether certain data should be shared is based on the goals the users have with regard to the target groups with whom the data is shared.

In [11], the study examined how users perceive the effects of using fitness trackers on their security and privacy. For this purpose, an online questionnaire was prepared in order to subsequently survey 212 users of fitness trackers in an online survey. The survey found that users take hardly any steps to protect the data collected by their fitness trackers from misuse. While they generally state that they know which data is collected by the fitness trackers, they were unsure about the possible uses of the collected data. The survey also queried various scenarios that show potential misuse with regard to the privacy and security of the data. These included scenarios such as identity theft through analysis of fitness data such as location data, or the recognition of individual users through analysis of their gait. While the surveyed users considered many of the scenarios shown to be possible, they found it unlikely that these would occur in reality.

3. Analysis

To analyse the security provisions of the Health Connect interface, an application was created that reads data from Health Connect. For this purpose, data from a body analysis scale was first written to the Health Connect database. The tool "openscale2HealthConnect" [12] was used to read the data from the scale's application and add it to Health Connect. This application transfers data on weight, body fat and total body water to Health Connect. The following describes which steps an application needs to take in order to read the data stored there. Since a potentially malicious application usually wants to read data that is already stored rather than write new data, the focus is on read access. The steps required to obtain write access are, however, similar to those for read access.

For an application to access the fitness and health data, the respective permissions must first be declared. As with any permission on Android, this is done in the application's manifest. This is an XML file that is part of the application package. In addition to information about the application, it declares the permissions requested by the application. These are identified by a unique designation (for example `android.permission.health.READ_BODY_WATER_MASS` for access to values of the category total body water). Depending on the type of permission, the system may grant it automatically merely through the declaration in the manifest. For many permissions, however, confirmation by the user is necessary before an application can use them. This is also required for all permissions for read or write access to Health Connect data.

Before the first access to Health Connect data, the application must actively request the desired permissions. To do so, the application creates a set with the permissions to be requested. This set is passed to the `HealthConnectClient`. This is the interface between the application and the Health Connect service running on the device. The `HealthConnectClient` then passes the requested permissions to the Health Connect service. The service then creates the permission dialog that is shown to the user. Such a permission dialog is shown in Figure 1. In this dialog, users have the option of allowing or denying access to individual data categories. The permission for access can be granted independently for write access and read access. In the figure shown, the application attempts to gain read access to the values body fat, weight and total body water. Granted permissions can be revoked by the user at any time in the device settings.

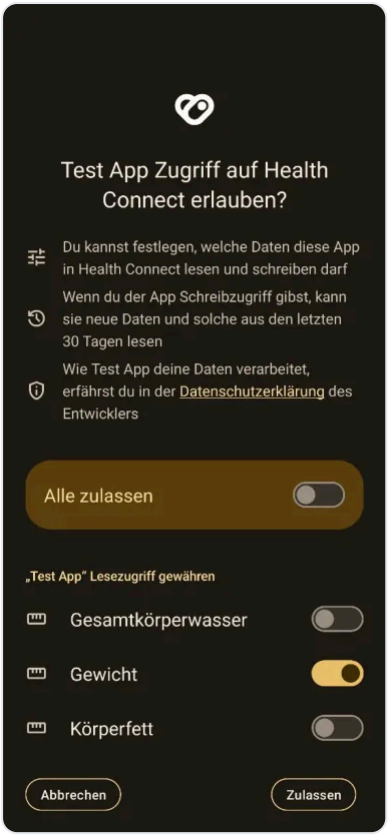


Figure 1: The Health Connect permission dialog allows users to release individual categories of fitness and health data for reading or writing by the requesting application.

To use Health Connect, an application absolutely needs a privacy policy. This must be declared in the application's manifest alongside the permissions. So that it can be displayed to the user, the application must declare its own activity that displays the privacy policy. This is launched via the action `ACTION_SHOW_PERMISSIONS_RATIONALE` when the user opens the privacy policy from the Health Connect settings dialog.

In addition to the technical prerequisites mentioned in the previous sections, access to Health Connect must be requested from Google for publication in the Play Store [13]. To do so, the developer must submit further detailed information in addition to general information about the application, such as name and package name, and information about themselves. This includes the use case of the application as well as a list of the requested permissions, justifications for why they are requested, and the developer's contact information. Similar to the application itself, these are reviewed by Google. However, detailed information about the review process is not available.

If an application fulfils all these prerequisites and the user agrees to access to the data, the application can use the Health Connect interface. To make verification easier for the user, every access by an application to Health Connect data is recorded. The list of accesses in the last 24 hours is visible in the Health Connect settings. An example is shown in Figure 2. In addition to the accessing application, the category of fitness and health data that was accessed is also shown.



Figure 2: Overview of the accesses to data in Health Connect.

4. Conclusion

This report showed which steps application developers must take in order to read data from the Health Connect interface on Android. For each category of values that is read, they must request the respective permission. When the application first accesses the interface, the user is asked for permission to access. The user has the option of releasing each category individually. A newly installed application also only has access to the data of the last 30 days. This should prevent a potentially malicious application from gaining access to all historical data. Applications that are offered via the Play Store must also have a mandatory privacy policy that explicitly addresses the processing of the data retrieved from Health Connect.

References

[1] Statista; IDC, „Wearables unit shipments worldwide from 2014 to 2022," 03 2023. [Online]. Available: https://www.statista.com/statistics/437871/wearables-worldwide-shipments/.

[2] Android Developers, „Android 14 - Health Connect," Google Inc, 2023. [Online]. Available: https://developer.android.com/about/versions/14/features#health-connect. [Zugriff am 27 12 2023].

[3] R. Pérez-Peñan und M. Rosenberg, „Strava Fitness App Can Reveal Military Sites, Analysts Say," The New York Times, 2018.

[4] K. Dhondt, V. L. Pochat, A. Voulimeneaso, W. Joosen und S. Volckaert, „A Run a Day Won't Keep the Hacker Away: Inference Attacks on Endpoint Privacy Zones in Fitness Tracking Social Network," in CCS '22: ACM SIGSAC Conference on Computer and Communications Security, Los Angeles, CA, USA, 2022.

[5] D. Lee, „MyFitnessPal breach affects millions of Under Armour users," BBC, 29 03 2018. [Online]. Available: https://www.bbc.com/news/technology-43592470. [Zugriff am 22 12 2023].

[6] Z. Whittaker, „Fitness app PumpUp leaked health data, private messages," ZDNet, 31 05 2018. [Online]. Available: https://www.zdnet.com/article/fitness-app-pumpup-leaked-health-dataprivate-messages/. [Zugriff am 22 12 2023].

[7] P. Muncaster, „Fitness App Kinomap Leaks 42 Million Records/," Infosecurity Magazine, 22 04 2020. [Online]. Available: https://www.infosecurity-magazine.com/news/fitness-app-kinomapleaks-42/. [Zugriff am 22 12 2023].

[8] C. Osborne, „Over 60 million wearable, fitness tracking records exposed via unsecured database," ZDNet, 13 9 2021. [Online]. Available: https://www.zdnet.com/article/over-60-million-recordsexposed-in-wearable-fitness-tracking-data-breach-via-unsecured-database/i. [Zugriff am 22 12 2023].

[9] „Unwinding Ariadne's Identity Thread: Privacy Risks with Fitness Trackers and Online Social Networksn," in MPS '17: Proceedings of the 2017 on Multimedia Privacy and Security, Dallas, Texas, USA, 2017.

[10] „"There is nothing that I need to keep secret": Sharing Practices and Concerns of Wearable Fitness Data," in USENIX, 2019.

[11] S. Gabriele und S. Chiasson, „Understanding Fitness Tracker Users' Security and Privacy Knowledge, Attitudes and Behaviours," in CHI '20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systemsl, 2020.

[12] bahuma20, „ openscale2healthconnect - Synchronize your data from the OpenScale app to Androids Health Connect framework," Github, 2023. [Online]. Available: https://github.com/bahuma20/openscale2healthconnect. [Zugriff am 27 12 2023].

[13] Android Developers, „Request access to Health Connect data types | Android health & fitness | Android Developers," Google Inc, 2023. [Online]. Available: https://developer.android.com/health-and-fitness/guides/health-connect/publish/requestaccess. [Zugriff am 27 12 2023].