35TH USENIX SECURITY SYMPOSIUM



Health Hazard, Handle with Care: Investigating the Privacy Risks of Android's Health Connect

Konstantinos Spyridakis · Ioannis Arkalakis · Michalis Diamantaris
Sotiris Ioannidis · Jason Polakis · Panagiotis Ilia

Technical University of Crete · University of Illinois Chicago · Cyprus University of Technology



THE LANDSCAPE

Health apps are growing in number, but

Increasingly sensitive data



App-specific data formats



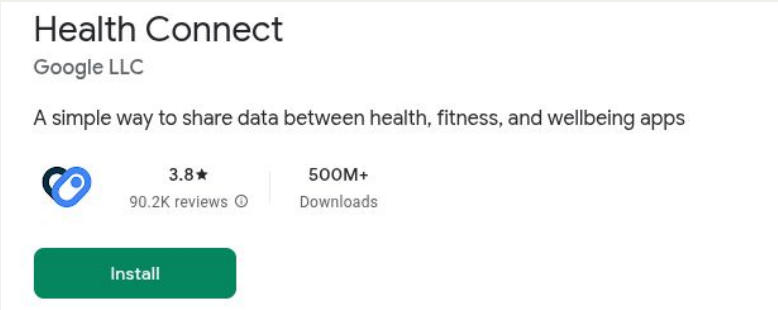
App-specific data sharing

Underscore the need for standardized managing and sharing of health data

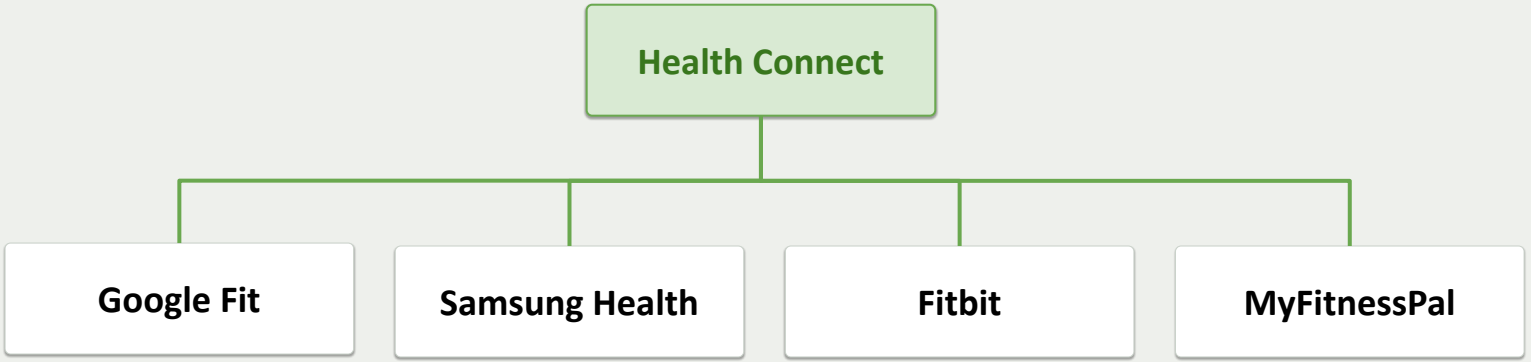
GOOGLE'S SOLUTION

OS support for managing and sharing health data

- 2022 launches as a standalone app



- 2023 folded into Android 14 as a system API

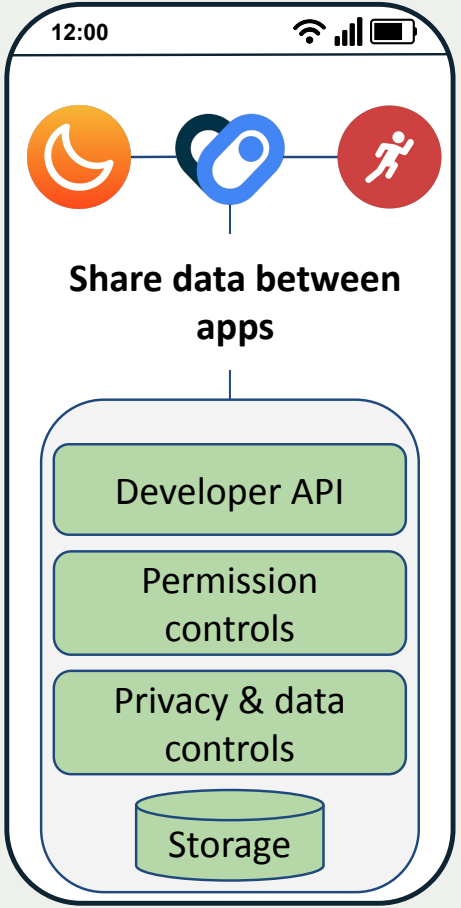


BACKGROUND

One database, every health app

Centralized on-device store

- Standardized schema for 50+ health and fitness record types
- Shipped as a standalone app, OS component
- Local storage

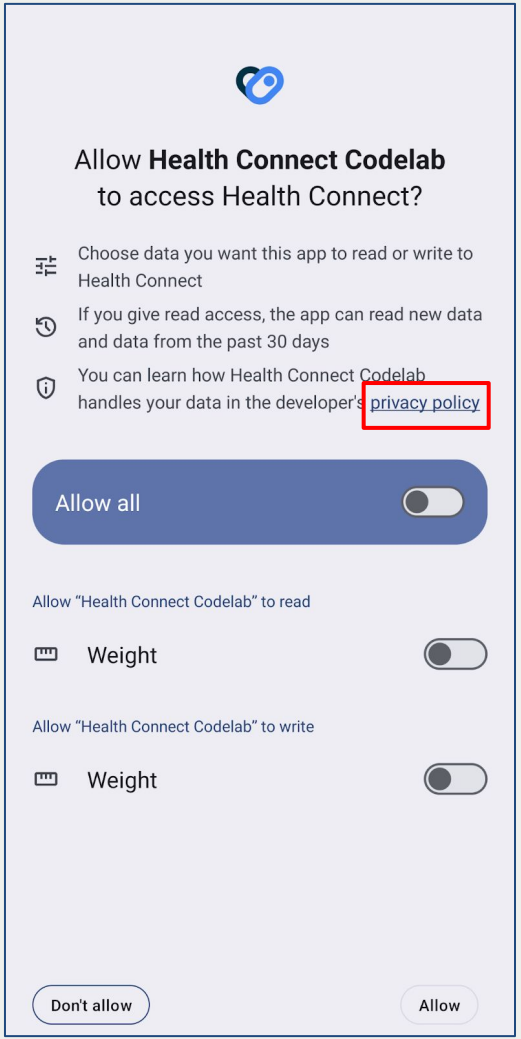


BACKGROUND

One database, every health app

Per-record-type permissions

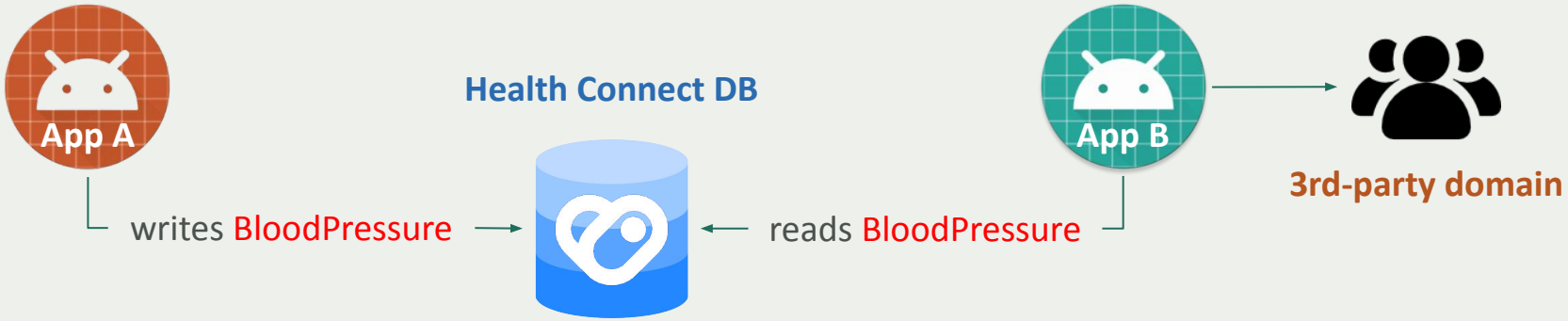
- declare *android.permission.health* in the Manifest
- show a permission rationale screen that links to their privacy policy



THE PROMISE

A centralized health database advertised as privacy-first by design

> *“Data is stored on-device, ensuring the user is in full control of their data.”*
>
> — Google, on Health Connect



We present the first empirical analysis of Android's Health Connect and uncover fundamental design flaws that expose users to significant privacy risks

METHODOLOGY

Dynamic cross-app analysis on a real device

Semi-manual pipeline intercepting cross-app data flows and correlating system and network logs to identify privacy risks and violations

PRIMING

- Grant all permissions
- 1st dataset of health connect records
- Populate database using custom app
- 5–15 min manual interaction, seeding with pre-defined records

→

PROBING

- Grant all permissions
- 2nd dataset of health connect records
- Populate database using custom app
- 5–15 min manual interaction, seeding with pre-defined records
- Trace health record flows

METHODOLOGY

End to end tracing for every Health Connect call

System monitoring

- Frida hooks on every health.connect.* class, applied recursively
- Binder-level interception — records move through IPC
- Reflection and parcel analysis to unpack raw serialized values
- Stacktraces attribute each call to first- or third-party code

Network monitoring

- Transparent BurpSuite proxy on a rooted Pixel 6
- SSL pinning, anti-root and anti-tamper checks bypassed
- Pre-seeded record values matched through GZIP, Base64, MD5, SHA256
- Candidate leaks verified manually

Semi-manual by design: precision over scalability.

DATASET

From 2.3 million apps down to 351

2,348,217

unique apps preprocessed from daily AndroZoo snapshots, Feb 2024 – Mar 2025

1,068

declare at least one Health Connect permission in their Manifest

351

actually invoke Health Connect APIs at runtime (final dataset)

11,504

records written by 91 apps stored in the device database after both phases ended

---

Excluded from analysis

361 required a membership · 283 never called Health Connect · 39 needed external hardware · 24 were paywalled · 10 failed to run, 5 of them using anti-analysis techniques

Testbed: Google Pixel 6 on AOSP 14, rooted with Magisk, real SIM for OTP

FINDINGS · TRANSPARENCY

What apps say versus what apps do

60.96%

fail the UI transparency guidelines

Rationale screen's policy link is missing or invalid

15.38%

never disclose that they collect health records

13.39%

never disclose that they share them

25.64%

disclose neither — 90 apps, leaving users unable to choose informedly

Privacy policies fare no better

- 6 apps ship no privacy policy at all
- 17 more never mention health data
- 3 apps state outright that they share or sell health data to advertisers

FINDINGS · TRANSPARENCY

What apps say versus what apps do

60.96%

fail the UI transparency guidelines

Rationale screen's policy link is missing or invalid

15.38%

never disclose that they collect health records

13.39%

never disclose that they share them

25.64%

disclose neither — 90 apps, leaving users unable to choose informedly

Privacy policies fare no better

- 6 apps ship no privacy policy at all
- 17 more never mention health data
- 3 apps state outright that they share or sell health data to advertisers

Strictly forbidden
even in aggregated anonymized form

FINDINGS · CROSS-APP ACCESS

Read by apps that never wrote the data

100 apps

28.49% of the dataset read 2,334 records created by other apps

4 apps

wrote ExerciseRoute records carrying GPS traces; three of those were read by five other apps

Scoped Storage bypass

- Covert-channel for cross-app communication and data exchange
- PNG image smuggled through a record's Title field

How far the reach goes

- 15.67% of apps read at least five records they did not create; 10% read at least twenty
- 17.37% pull data originating from four or more different apps
- Sensitive types are in scope: sexual activity, ovulation tests, menstruation flow and periods

FINDINGS · EXFILTRATION

Off-Device data exposure

69 apps

19.60% transmit Health Connect data off-device

481 values

leaked by a single app, with none of it declared in its Data Safety shared section

13 apps

leak other apps' package names — six of them between 14 and 69 names each

What leaves the phone

- **ExerciseSession Title and Notes** : leaked by 32 and 26 apps, enough to build a distinct fitness profile
- **15 apps leak nutrition detail :** three leak vital signs such as blood pressure and body temperature

REAL-WORLD SCENARIOS

This isn't hypothetical

Fitness data to Google Ads

DIRECT VIOLATION

MyFitnessPal **leaked exercise data** and **device identifiers** to Google's advertising domain

Metadata fingerprinting

13 APPS

Leaked package names reveal sensitive health information, allowing accurate user identification and health condition inferences

Health record transmission via shady techniques

NO CONSENT

A weight-tracking app **transmitted** a **screenshot** containing sensitive health data to *ingest.sentry.io*

Health insurance apps

INSURANCE & PRIVACY

Six apps **accessed/exfiltrated PII** and showed potential Health Connect health data access, raising privacy concerns due to inconsistent data disclosures

Flo Health

$56M SETTLEMENT

- *OvulationTest.result* and *CervicalMucusRecord.appearance* plus timestamps, sent them to its backend, and disclosed only "fitness" data
- Deceptive data-sharing practises → Google & Flo's Sept 2025 FTC settlement

REAL-WORLD SCENARIOS

This isn't hypothetical

Fitness data to Google Ads

DIRECT VIOLATION

MyFitnessPal **leaked exercise data** and **device identifiers** to Google's advertising domain

Forbidden

Metadata fingerprinting

13 APPS

Leaked package names reveal sensitive health information, allowing accurate user identification and health condition inferences

Health record transmission via shady techniques

NO CONSENT

A weight-tracking app **transmitted** a **screenshot** containing sensitive health data to *ingest.sentry.io*

Health insurance apps

INSURANCE & PRIVACY

Six apps **accessed/exfiltrated PII** and showed potential Health Connect health data access, raising privacy concerns due to inconsistent data disclosures

Flo Health

$56M SETTLEMENT

- *OvulationTest.result* and *CervicalMucusRecord.appearance* plus timestamps, sent them to its backend, and disclosed only "fitness" data
- Deceptive data-sharing practises → Google & Flo's Sept 2025 FTC settlement

REAL-WORLD SCENARIOS

This isn't hypothetical

Fitness data to Google Ads

DIRECT VIOLATION

MyFitnessPal **leaked exercise data** and **device identifiers** to Google's advertising domain

Forbidden

Metadata fingerprinting

13 APPS

Leaked package names reveal sensitive health information, allowing accurate user identification and health condition inferences

Health record transmission via shady techniques

NO CONSENT

A weight-tracking app **transmitted** a **screenshot** containing sensitive health data to *ingest.sentry.io*

without user's knowledge/consent

Health insurance apps

INSURANCE & PRIVACY

Six apps **accessed/exfiltrated PII** and showed potential Health Connect health data access, raising privacy concerns due to inconsistent data disclosures

Flo Health

$56M SETTLEMENT

- *OvulationTest.result* and *CervicalMucusRecord.appearance* plus timestamps, sent them to its backend, and disclosed only "fitness" data
- Deceptive data-sharing practises → Google & Flo's Sept 2025 FTC settlement

DEEP DIVE

The app you cannot turn off

READ_HEALTH_DATA_IN_BACKGROUND

Read the database while the app is not open

READ_HEALTH_DATA_HISTORY

Read the entire history, past the default 30-day window

Weight Loss Tracker Noyoy app requests both permissions:

- Reads 50 other apps records and transmits them with the user's email, age, carrier
- Swiping the app away does not stop collection, only a force-stop from system settings does

---

11 more apps hold background access — seven read records belonging to other apps, and two leaked them alongside the user's email and full name.

FIXING IT

Provenance and purpose, not just permission

1 **Context-aware access control**

Authorize on provenance, not just record type

⟨ requesting_app, record_type, originating_app, purpose, timeframe ⟩

2 **Purpose-bound data access**

Every cross-app access declares an explicit purpose — similar to the Data Safety location-permission rationale

3 **Automated vetting**

Static + dynamic checks in Play review to catch undisclosed collection prior to app release

FIXING IT

Disclosure and Response

1 Google confirms our findings, demonstrated results enable targeted investigation

2 Policy violations confirmed

- Health data sharing with advertising domains
- Unauthorized screen-content capture by analytics SDKs
- Inconsistencies between declared and actual data practises

3 Enforcement

- Enforcement actions were initiated against a subset of non-compliant apps

4 Contribution

- Improve review and detection mechanisms
- Mitigate covert channel for cross-app data exchange (i.e., “Title” field)

CONCLUSION

Remarks

1. **Health Connect introduces significant privacy risks,** despite its goal of improving user control

2. **Real-worlds apps** were found accessing and exfiltrating sensitive health data **without the user's consent, violating Google's policies and guidelines**

3. **Design improvements and stronger policy enforcement are essential** and **CRITICAL** when it comes to future medical records

Thank you!

ARTIFACT



no health data
collectedduring
scanning...probably

kspyridakis1@tuc.gr

TECHNICAL UNIVERSITY OF CRETE
UNIVERSITY OF ILLINOIS CHICAGO
Cyprus University of Technology

Icons made by Flaticon