January 2020

Health and Activity Evidence

How smartphones and trackers collect and store health data, and how to obtain health information

Vladimir Katalov, ElcomSoft

Your device is a source of evidence

- Pictures and videos
- Location history, routes and places
- Third-party app data
- Cached internet data
- System and application logs
- Social network activities
- Health and activity data
- Comprehensive device usage stats
- Contacts & calendars
- Call logs and text messages
- Emails and chats
- **Account and application passwords**
- **Web and Wi-Fi passwords**
- Documents, settings and databases
- Web history & searches

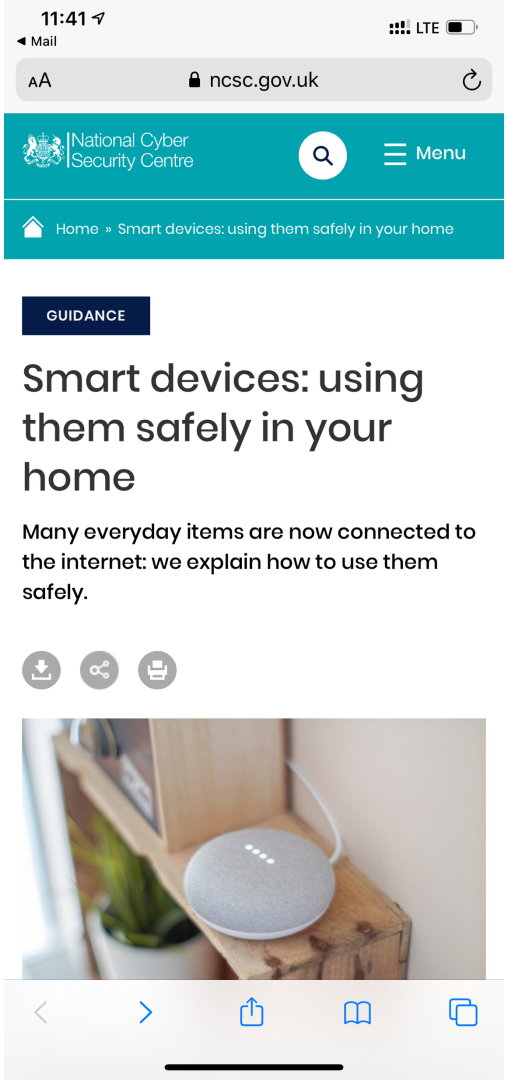
Your device is a source of evidence

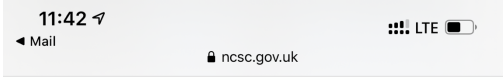
- **It's not just about the device**
  - The OS manufacturer (Google, Apple) collects and processes tremendous amounts of data in the cloud
- **It's not just the OS manufacturers**
  - Device OEMs (Samsung, Huawei, Xiaomi etc.) also collect and process data
- **Not even just them…**
  - Third-party apps and services have their own cloud accounts
  - Strava, Microsoft apps, Facebook etc.

NCSC guidance

Smart devices: using them safely in your home (Feb 15, 2019)

https://www.ncsc.gov.uk/guidance/smart-devices-in-the-home





What is the risk from using Smart Devices?

Just like a smartphone, laptop or PC, smart devices can be hacked to leave your data and privacy at risk. Very rarely, devices have been controlled by somebody else managing the device, often to frighten the victim.

- Children's GPS and fitness trackers (BBC News)
- Security cameras could be hijacked (BBC News)
- Smart home gadgets in domestic abuse warning (BBC News)

The NCSC and DCMS are encouraging manufacturers to make (and keep) their products secure, and have developed a code of practice (PDF) to help keep consumers safe. There's also lots you can do to protect yourself.

Setting up your device

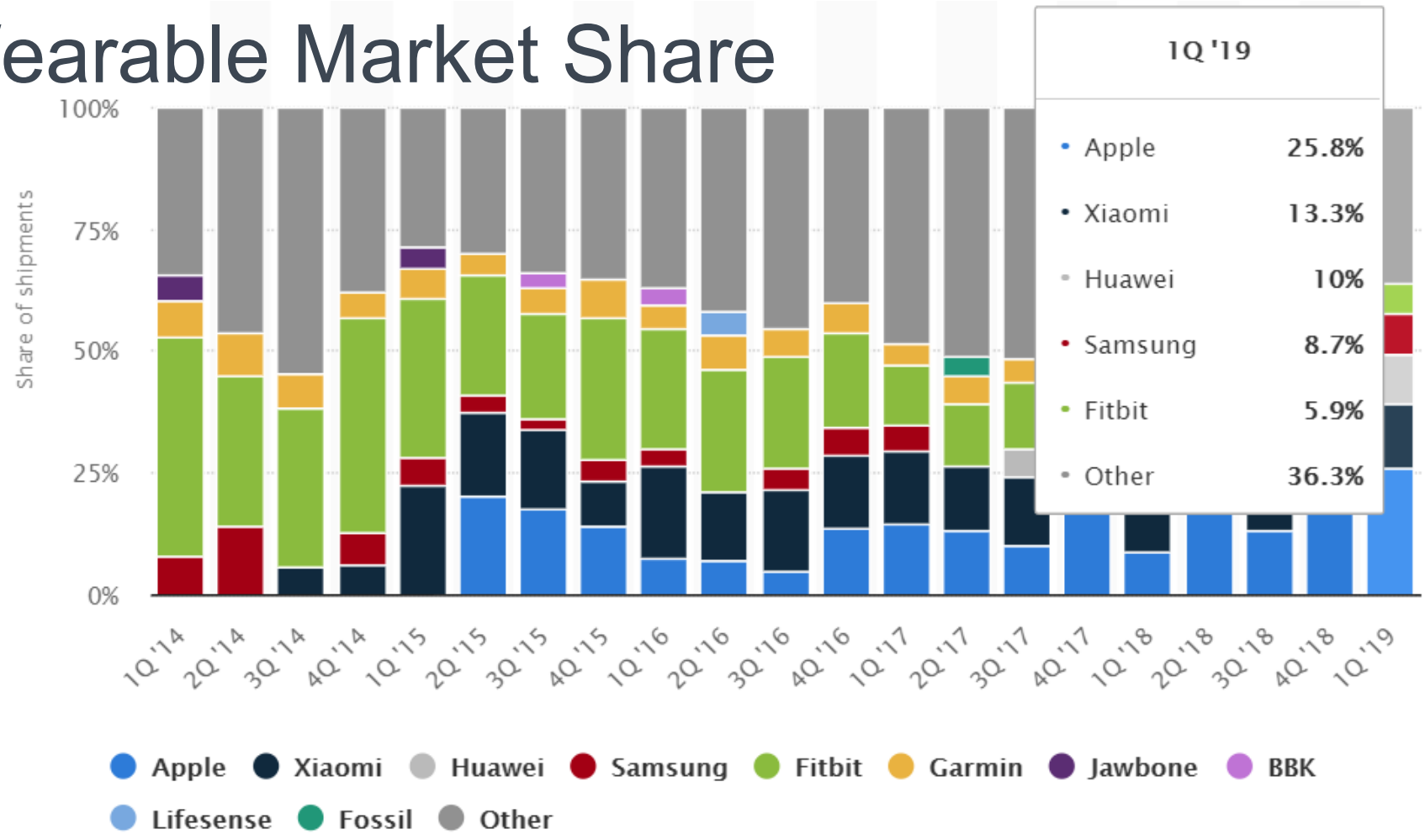
Back to top

heck reviews of the

Most of that data ends in the cloud

- **Apple iCloud**
  - Backups, files, photos, synchronized data, point-to-point encrypted data (including Health and passwords)
- **Google**
  - Massive amounts of synchronized data; location history; passwords; search history; Google Fit; backups
- **Others**
  - Often massive collection of data is poorly disclosed and poorly documented

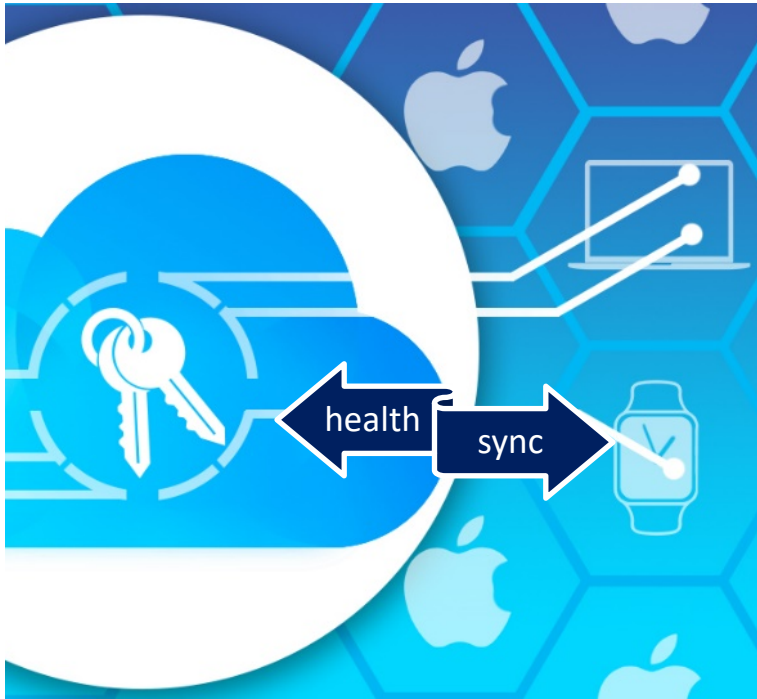
Wearable Market Share



Health Evidence

Health evidence is stored in the cloud

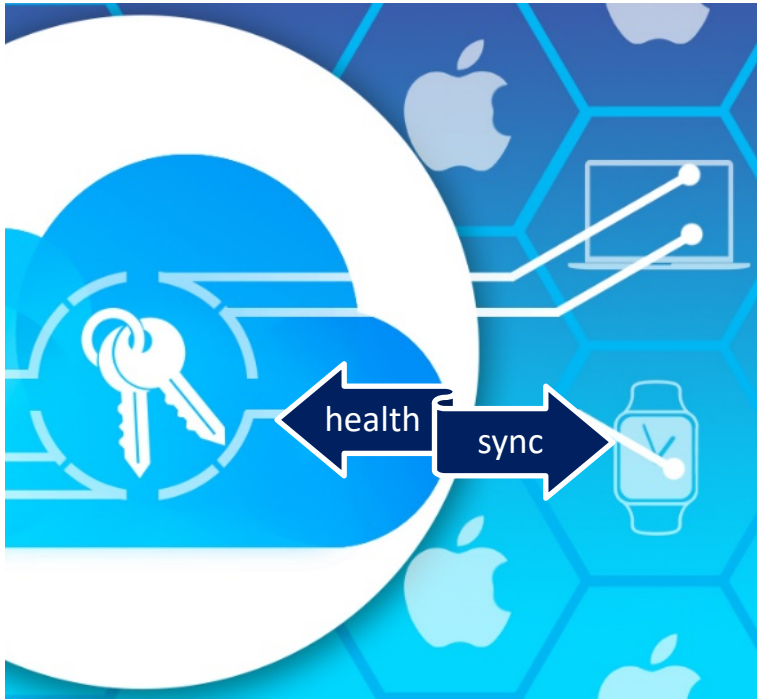
- **Apple and Google cloud platforms**
- Single point access to all health data is very tempting
- Some manufacturers sync Health data, and some don’t
- Apple requires sharing data with Apple Health to approve manufacturer’s HealthKit integration
  - Some manufacturers ignore HealthKit altogether
- Google does not have any requirements
  - Most manufacturers ignore Google Fit



Health Evidence

Apple Watch, Google WearOS (ex- Android Wear)

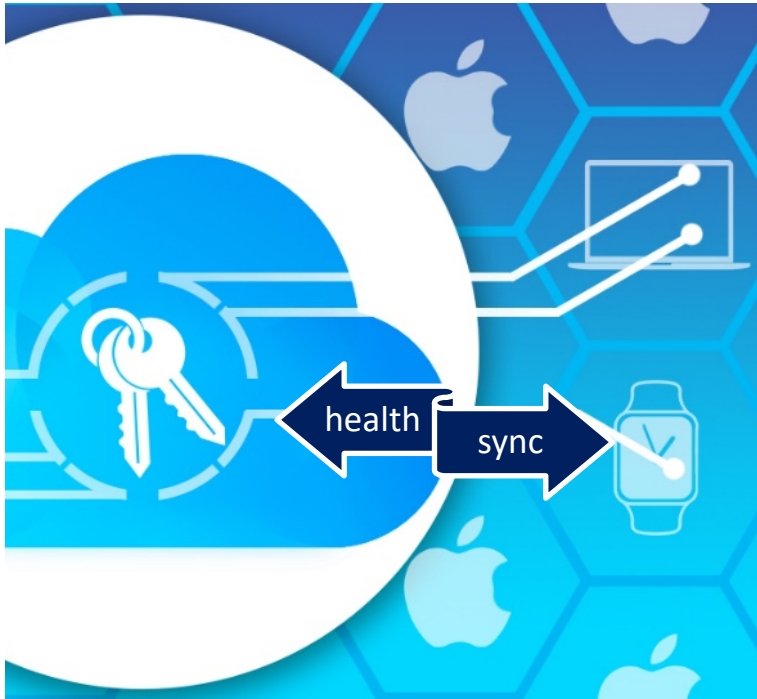
- **Apple Watch:** iCloud only
  - Exclusively works through Apple HealthKit
  - **No** integration with Google or Android
- **Google WearOS watches** (all models)
  - Works on iOS devices, but…
  - **No** integration with Apple HealthKit (Google's decision)
  - Full integration with Google Fit



Health Evidence

Fitness trackers with proprietary cloud services

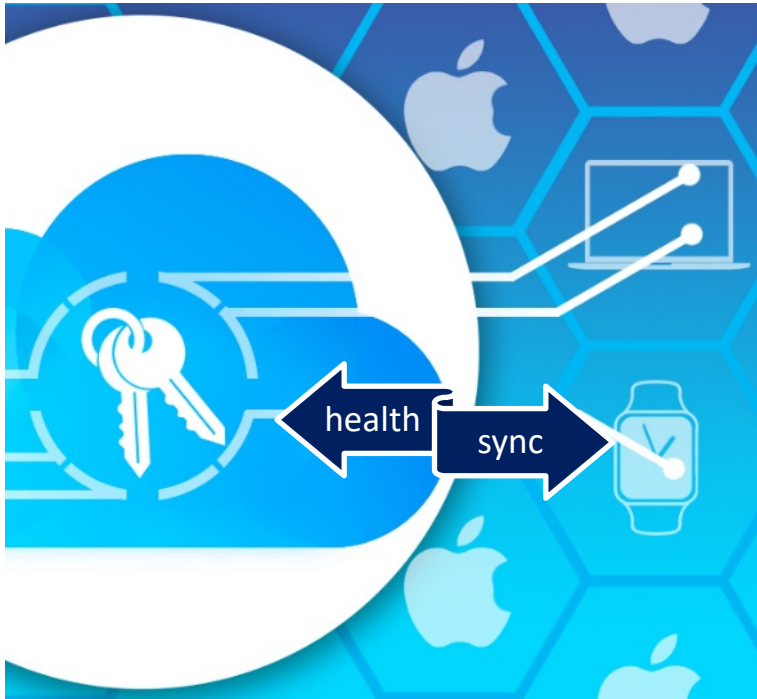
- **Samsung Health: proprietary Samsung Cloud**
  - Ignores Apple HealthKit and Google Fit
- **Xiaomi, Amazfit**: Mi Cloud, proprietary cloud
  - Integration with Apple HealthKit
  - Google Fit: limited (steps only) integration



Health Evidence

Fitness trackers with proprietary cloud services

- **Garmin**: Garmin Connect, proprietary cloud
  - One-way sync > to Apple HealthKit
  - Google Fit: no integration
- **Fitbit: proprietary cloud only**
  - Ignores Apple HealthKit and Google Fit



Apple Health and Apple Watch

The Number One Health Tracker

- Apple Watch is the number one health tracking device
- 25.8% market share in Q1’2019
- Apple Watch is an essential part of Apple Health, but…
- Apple Health works with or without the Apple Watch
- Uses iPhone low-energy sensors to collect fitness data

Apple Health

What Is Apple Health?

- Introduced in Sep 2014 with iOS 8
- Health app pre-installed on all iPhones
- Makes use of low-energy sensors
- Always active, always collecting information
- Supported by Apple Watch, additional data collected

Apple Health

Main Data Categories

- **Activity** – how much you move
- **Nutrition** – breakdown of your diet
- **Sleep** –your sleep habits
- **Mindfulness** – native support limited to Mindful Minutes, Activity and Sleep; third-party apps help build out your mindfulness data. Pretty meaningless in its current state, may improve in iOS 12 (have not checked yet)

Apple Health

Additional Data Categories

- **Body Measurements** – height and weight
- **Health Records** - CDA + Health Records
- **Heart** – blood pressure, heart rate
- **Reproductive Health** – sexual activity and menstruation cycles
- **Results** – various medical test results (e.g. sugar level)
- **Vitals** – blood pressure, body temperature, heart rate, breathing rate
- **Medical ID** – essential medical data

Apple Health

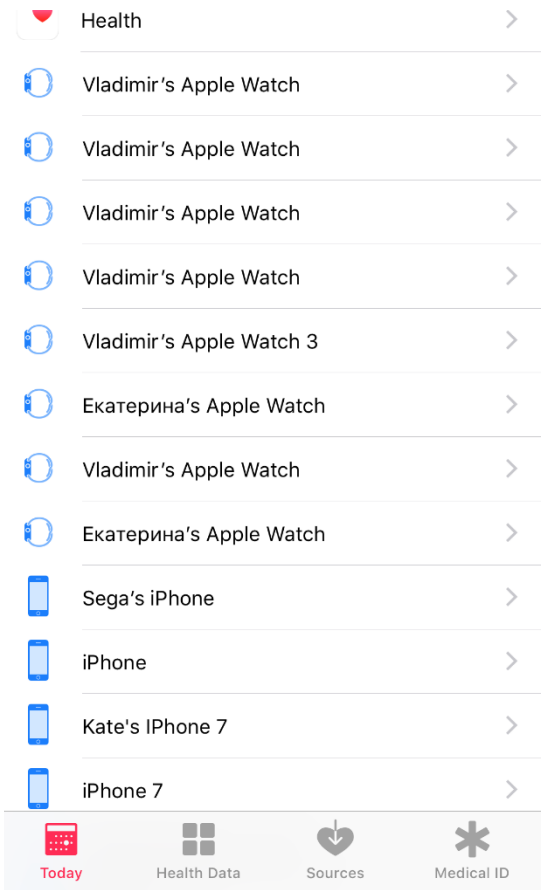
Where Apple Health Gets Data From

- Manual entry in the Health app
- Data received from HealthKit devices (iPhone, Apple Watch, compatible fitness trackers etc.)
- Third-party apps (Nike+, Strava, Workouts++)

Apple Health

Where Apple Health Gets Data From

- Data received from HealthKit devices (iPhone, Apple Watch, compatible fitness trackers etc.)
  - Automatic data submission
  - Pulse, blood pressure
  - Data for Mindfulness, Heart and Activity
  - Apple Watch collects Sleep data; **no automatic mode** (third-party apps can be used)



Apple Health

Apple Watch

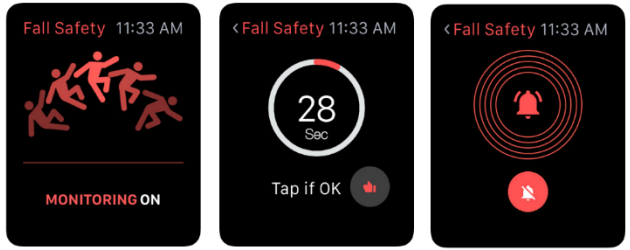
- Apple Watch contributes greatly to Health data
- Compatible with third-party apps (e.g. Pedometer++, Runkeeper)
- Steps (Health app calculates distance travelled)
- Heart rate
- Basic activity info: how long you stand, how much you exercise, calories burned
- New: Apple Watch 4 supports ECG (Electrocardiogram) (US only)

Apple Health

Apple Watch

- New: Fall detection
- Three fall patterns
- Automatic call to emergency number
- Logs and syncs fall events
- Essential bit of evidence: exact timestamp (down to the second) of the crime
    - Synced with the cloud, data may be available even if phone and watch are taken from the victim

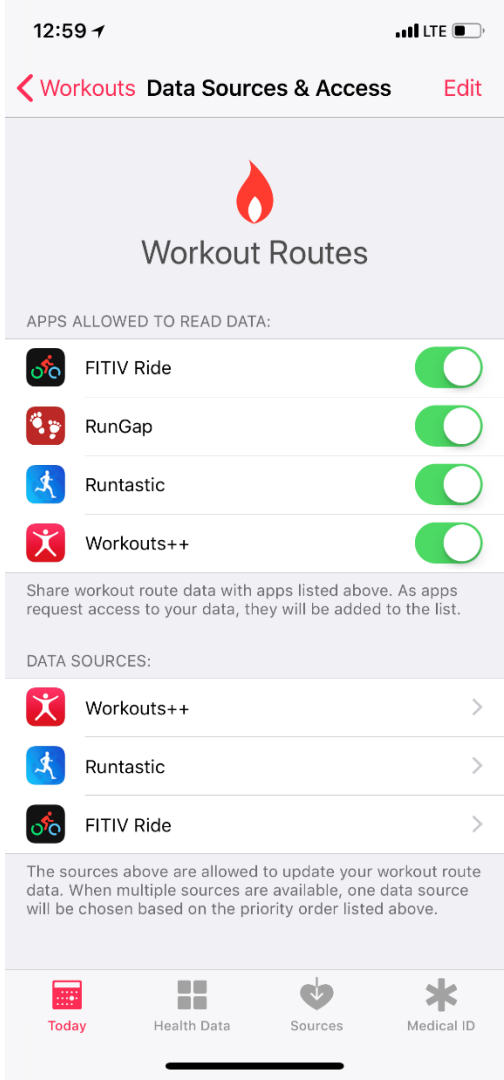
Apple Watch



Apple Health

Third-party apps as source of health data

- Third-party apps (Nike+, Strava, Workouts++)
  - All data categories supported
  - Except Health Records and Medical ID
  - Each data category has a list of “Recommended” third-party apps for collecting that type of data
  - Third-party apps must be activated in categories tracked in Health > Sources



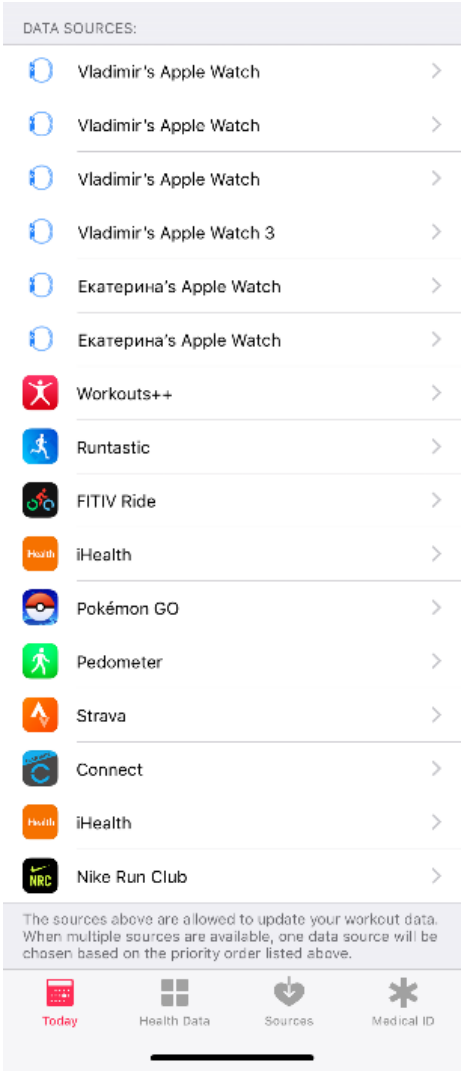
Apple Health

Apple Watch and Health security

Apple Health

How Apple Health Data Is Stored

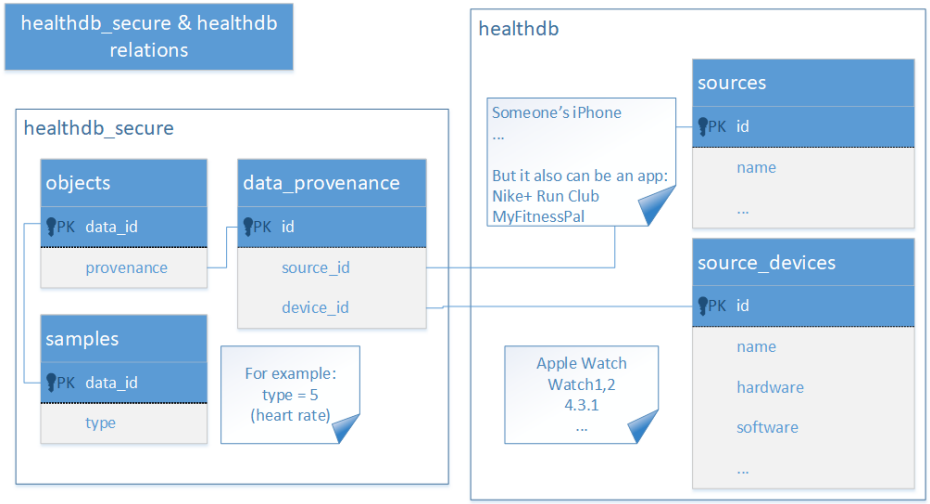
- Main data stored at **/private/var/mobile/Library/Health/**
- Two linked SQLite databases: **healthdb.sqlite** and **healthdb_secure.sqlite**
- Training geodata (?): **healthdb_secure.hfd** (encrypted)



Apple Health

Database Structures

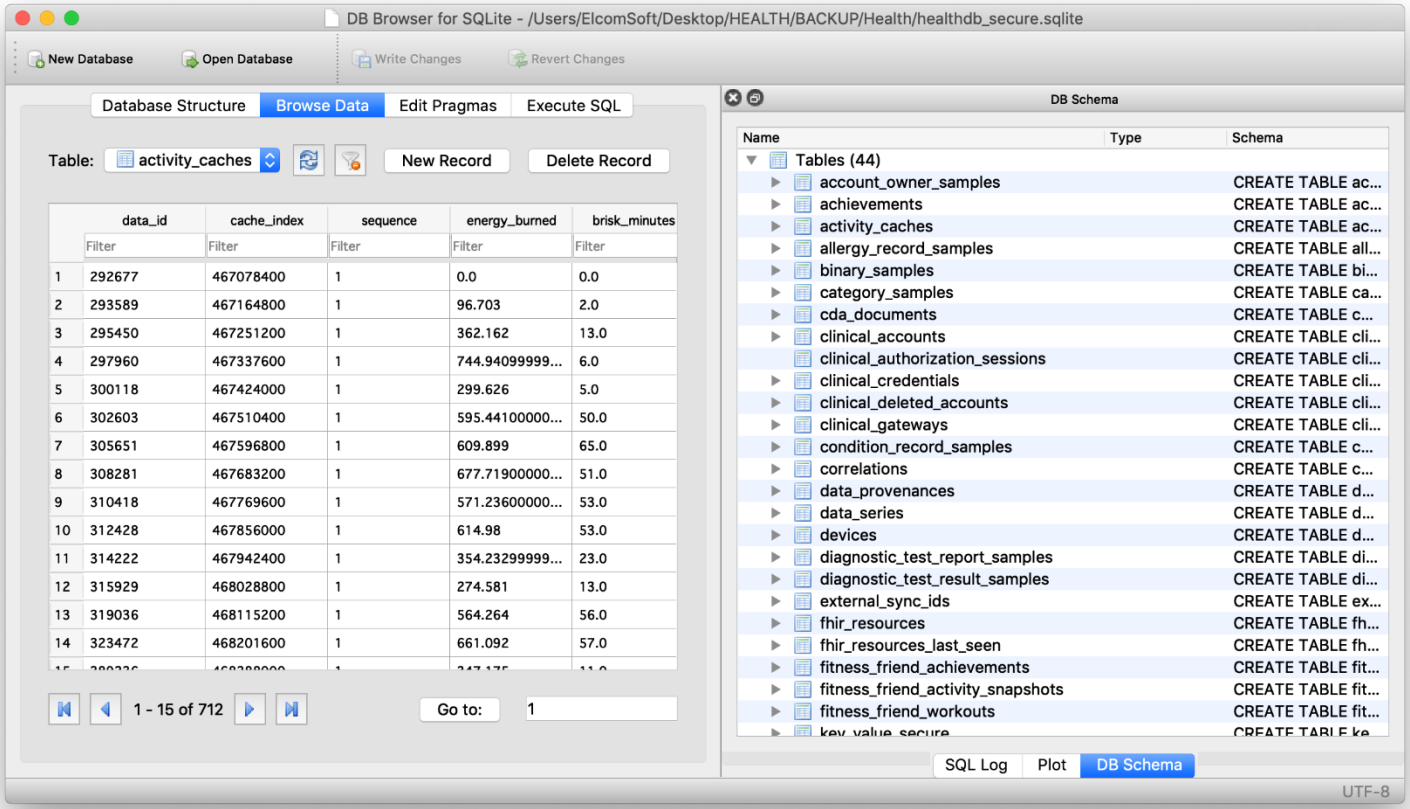
- healthdb.sqlite mainly contains information about data sources
- healthdb_secure.sqlite stores basic health information with frequent links to the first DB



Prior work

A Forensic Exploration of iOS Health Data (Heather Mahalik)
https://www.sans.org/summit-archives/file/summit-archive-1528385073.pdf

Apple Health



Apple Health

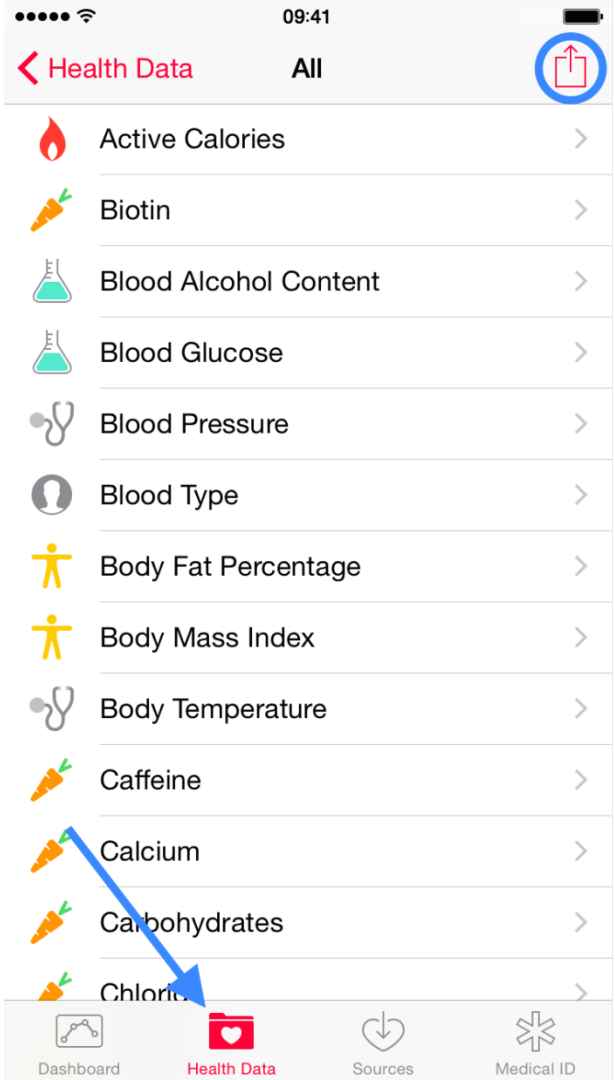
Accessing Apple Health Data

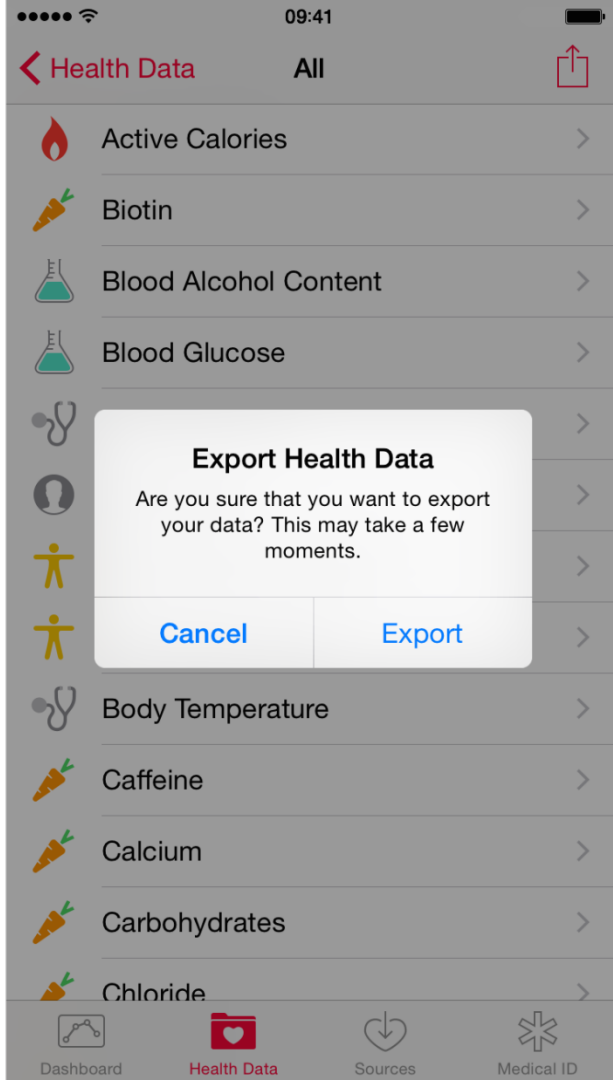
- Export from Health app (XML)
- Local backup (encrypted only)
- File system acquisition (requires jailbreaking)
- GDPR request
- Government/LE request
- Cloud extraction

Apple Health

Exporting Data

- Apple Health has export option
- Data can be exported to a ZIP file (with two XMLs)
- Analysis?





Apple Health

Extracting Apple Health Data: The Easy Way

- Apple Health is available via logical acquisition
- **No Apple Health data in unencrypted backups!**
  - Unlike keychain, which is still present in unencrypted backups, protected with a hardware key
- Set a known password before making a backup
- Make local backup with iTunes
- Decrypt backup, access Apple Health data
- View with forensic software (or analyse databases manually)

Apple Health

Extracting Apple Health Data: The Complex Way

- Apple Health is available via file system acquisition
- **Jailbreak required**
  - At this time, jailbreak is available for all versions of iOS from 8 to 11.3.1
- Jailbreak, use ssh (or forensic software)
- Obtain TAR image
- View with forensic software (or analyse databases manually)
- *Needed only if backup if password-protected*

Apple Health

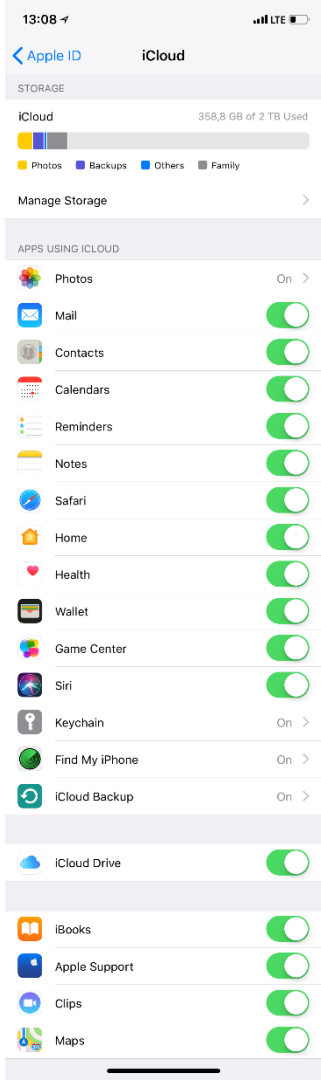
Extracting Apple Health Data: GDPR

- EU users can access their Health data by pulling a GDPR request
- Registering GDPR request: **privacy.apple.com**
- **Apple ID, password, 2FA required**
- Takes up to 7 days to receive the data
- Multiple binary and text formats

Apple Health

Apple Health and Cloud

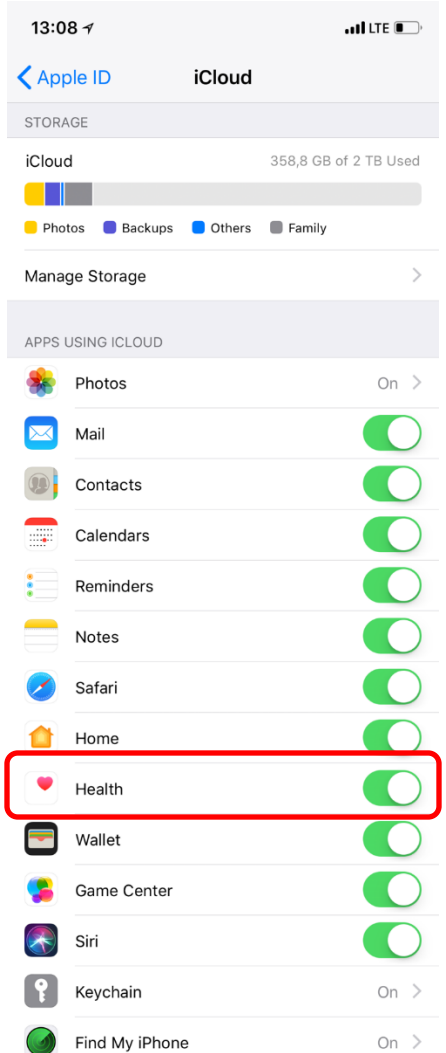
- Native Apple Health data is synced with iCloud to all registered devices
- Third-party apps operate through HealthKit
- Some third-party app data is not shared with Apple Health
- Certain apps use proprietary cloud sync (Strava, Endomondo)
- **Medical ID** data is unique per device and **does not sync**
- **CDA records** do not sync (to the best of our knowledge)



Apple Health

Apple Health and iCloud

- Apple Health data **can** be obtained from iCloud
- May contain significantly more information compared to what is available on device
- Technically, Apple Health belongs to “synced data” as opposed to “cloud backups”
  - This results in significantly more reliable extraction
  - Loose expiration rules of iCloud tokens compared to backups



Apple Health

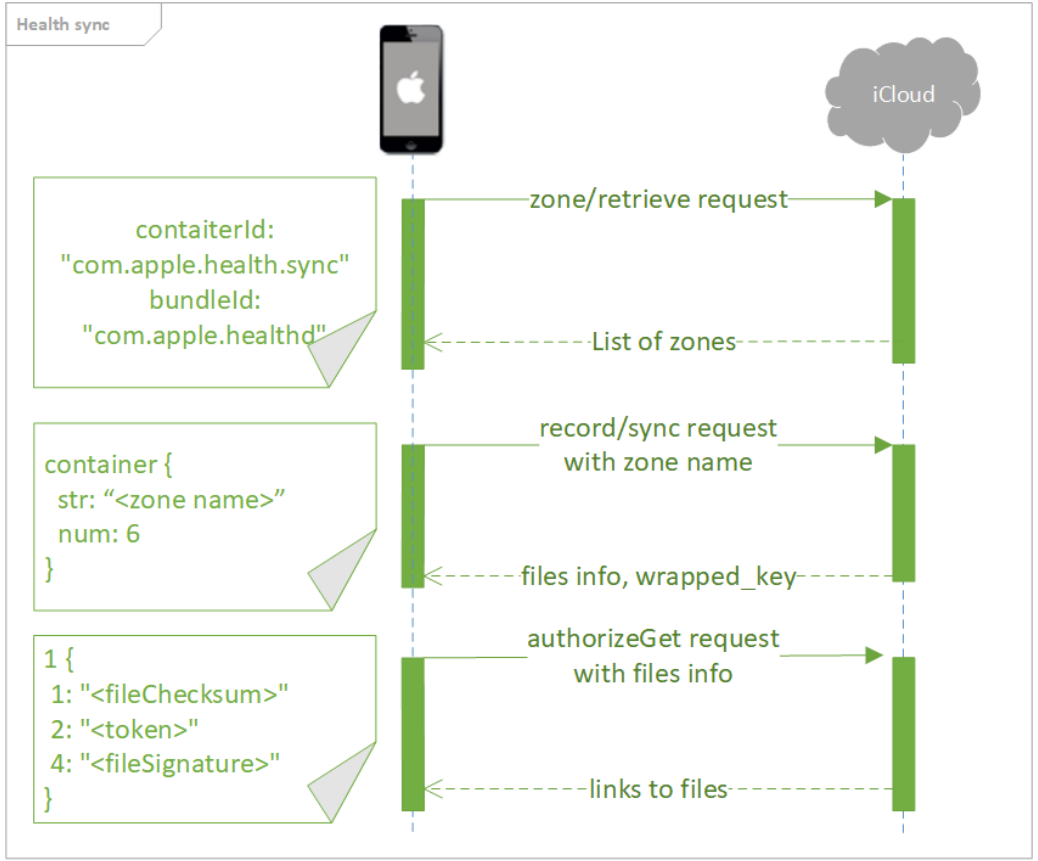
How Apple Health Data Is Synced

- Regular syncing: scheduled, after device reboot, on account change
- Data is stored in iCloud Drive (in chunks)
- Unlike iCloud Keychain or Messages, iCloud Health data has no additional protection
    - No need to enter device passcode, no additional encryption

Apple Health

Accessing Health Data

- Receive encrypted file chunks
- Request zone list
- Request zone sync
- Request file links
- Download files



Apple Health

```
containerId: "com.apple.health.sync"
bundleId: "com.apple.healthd"
```

Request Zone List

- All zones start with PrimarySyncCircle
- Followed by zone UUID, e.g. 1AA8B4D0-9B73-4D88-A740-BFE04DD8A5AC
- New zones created with logging in or on subsequent logins
- Zones are periodically merged

Apple Health

Request Zone Sync

- Request / Result:

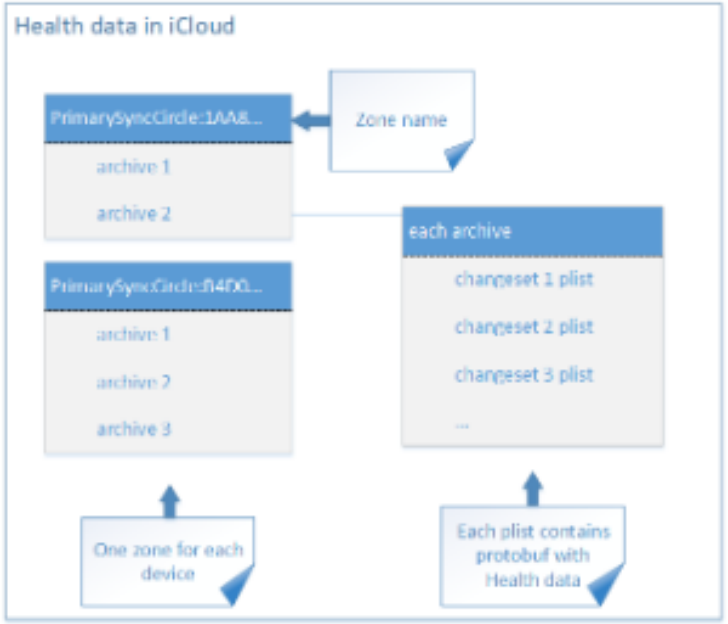
```
container {
 str: "PrimarySyncCircle:AF64D6
29-3688-4062-9503-BE97B45D5BC2"
 num: 6
}
```

```
propertyName {
 name: "ChangeSet"
}
propertyValue {
 valueType: 6
 authInfo {
  owner1Dsid: "8888888888"
  fileChecksum: "\001\233\254\2671GQ\316\324mM\243\031\254\322|\017\364\233N\
f"
  structSize: 13465
  token: "B3B9SvMwRNXBK6fGaX6vOuVLwfbWA1H5QwEAAAMR7kM"
  url: "https://p29-content.icloud.com:443"
  owner2Dsid: "8888888888"
  wrapped_key {
   name: "\003_\242\000\335\266\255\312\0304\226e\344\333\235\227\226a\266\32
3H\364\021DM3\341\020~B\337O\346\016\017\357\375C[\346\301\311\356\261"
  }
  fileSignature: "\001\310\273\331\332\326a\337\202Xd\035e`p\277\321\226\211\
222\312"
  downloadTokenExpiration: 1529588220
 }
}
```

Apple Health

Download Files

- Files from the list are downloaded by chunks
- Downloaded chunks must be decrypted
- record/sync request returns encrypted key (wrapped_key)
- Key is decrypted
- We’ve got a key for unwrapping encryption keys that accompany each chunk
- These keys are unwrapped with wrapped_key and are used to decrypt the chunks
- Decrypted chunks are merged into files



Apple Health

Sounds too simple?

- Synced data is received in protobuf structures
- Received structures are serialized objects described in HealthDaemon header files
- There are several types of Protobuf structures

```
@interface HDCodableObject : PBCodable <HDDecoding, NSCopying> {
        double _creationDate; //proto index 4
        long long _externalSyncObjectCode; //proto index 5
        HDCodableMetadataDictionary* _metadataDictionary; //proto index 2
        NSString* _sourceBundleIdentifier;
        NSData* _uuid; //proto index 1
        SCD_Struct_HD20 _has;
}
@interface HDCodableSample : PBCodable <HDDecoding, NSCopying> {
        long long _dataType; //proto index 2
        double _endDate; //proto index 4
        double _startDate; //proto index 3
        HDCodableObject* _object; //proto index 1
        SCD_Struct_HD48 _has;
}
@interface HDCodableCategorySample : PBCodable <HDDecoding, NSCopying> {
        long long _value; //proto index 2
        HDCodableSample* _sample; //proto index 1
        SCD_Struct_HD16 _has;
}
```

Apple Health

Accessing Health Data in iCloud

We can download **synced data**, which includes Apple Health

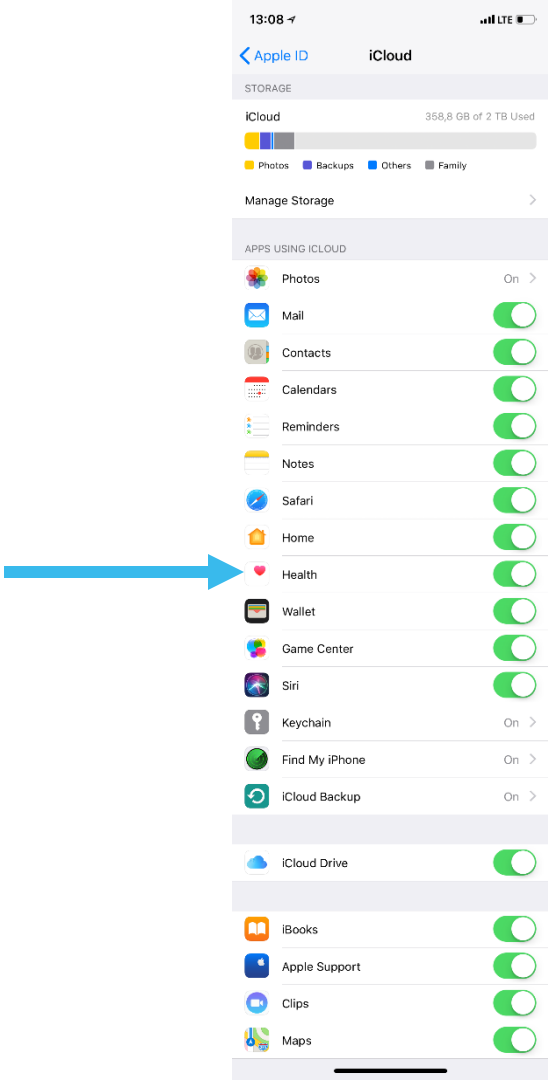
What can go wrong:

- Two-factor authentication may be an issue
- Access to secondary authentication factor is required (unless using authentication token)

Apple Health

iCloud Data Sync

- Health data
- If Settings | iCloud | Safari is enabled, it syncs:
  - Bookmarks
  - Open tabs
  - Reading list
  - Browsing history
- **Call logs** (not in the Settings; syncs if iCloud Drive is enabled)
- Contacts, Notes, Calendars, Wallet (including boarding passes), Maps (searches and bookmarks, routes)
- Keychain (device passcode required)
  - With luck, password to Google Account
- Messages (iMessages, SMS): since iOS 11.4 (keychain required)
- Third- party apps data



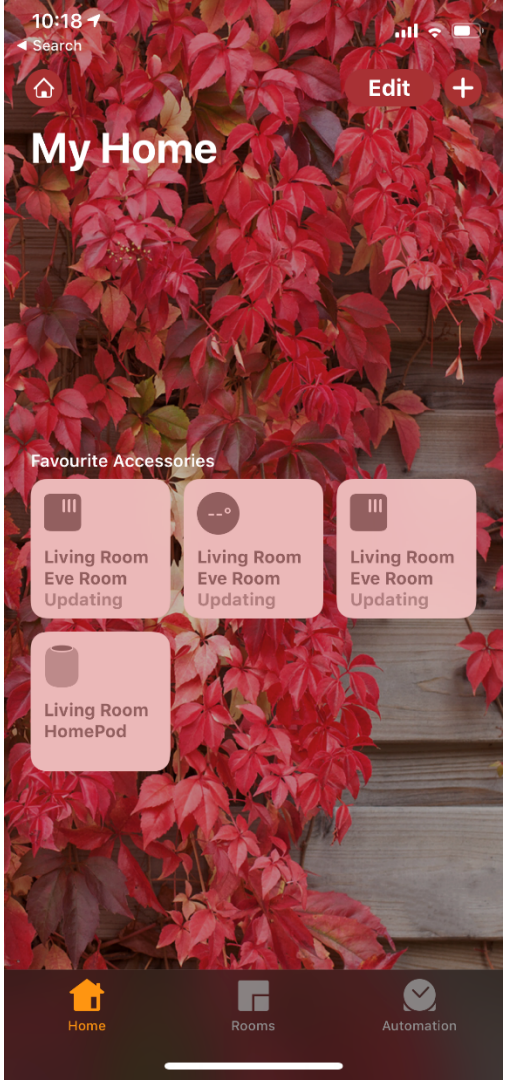
Apple Health

iCloud: what's next?

More synced data in iCloud

- Home data (HomePod, various sensors, lights, thermostats etc)
- Screen Time (app usage; previously available via full file system acquisition only)
- Voice memos
- Weather & Stocks

Remember Celebgate? ;)



Google Fit

Data collected by Google Fit

- **Activity**: active minutes, activity segments, heart points, sessions (workouts), walking and running, steps, Location
- **Body Measurements**: height and weight
- **Heart**: heart rate and blood pressure
- **Nutrition**: carbohydrates, cholesterol, dietary energy, dietary fiber, protein, saturated fat, sodium, total fat, caffeine, calcium, monounsaturated fat, polyunsaturated fat, potassium, sugar, etc.
- **Sleep**: sleep data
- **Sensors**: raw timestamped sensor data

Google Fit

Where Google Fit data is stored

- Google collects Fit data only if the **optional** Google Fit app is installed from Google Play store
- The app collects and syncs Fit data with Google Drive
- Health data is stored in Google Drive with no additional protection
- Can be exported via Google Takeout, extracted with Elcomsoft Cloud Explorer or requested by LE
- Can be downloaded with updated Elcomsoft Cloud eXplorer (ETA: Q1’2020)

Google Fit vs. Apple Health

The two systems compared

- A third-party fitness tracker or smart watch device supporting both Android and iOS is more likely to share data with **Apple Health** rather than **Google Fit**
- Apple Health standardizes data. HealthKit compliant apps cannot supply types of data that are not defined by Apple.
- Google Fit will accept data of any type including unknown. Unknown types of data will not be displayed but will be synced in the cloud.

Google Fit vs. Apple Health

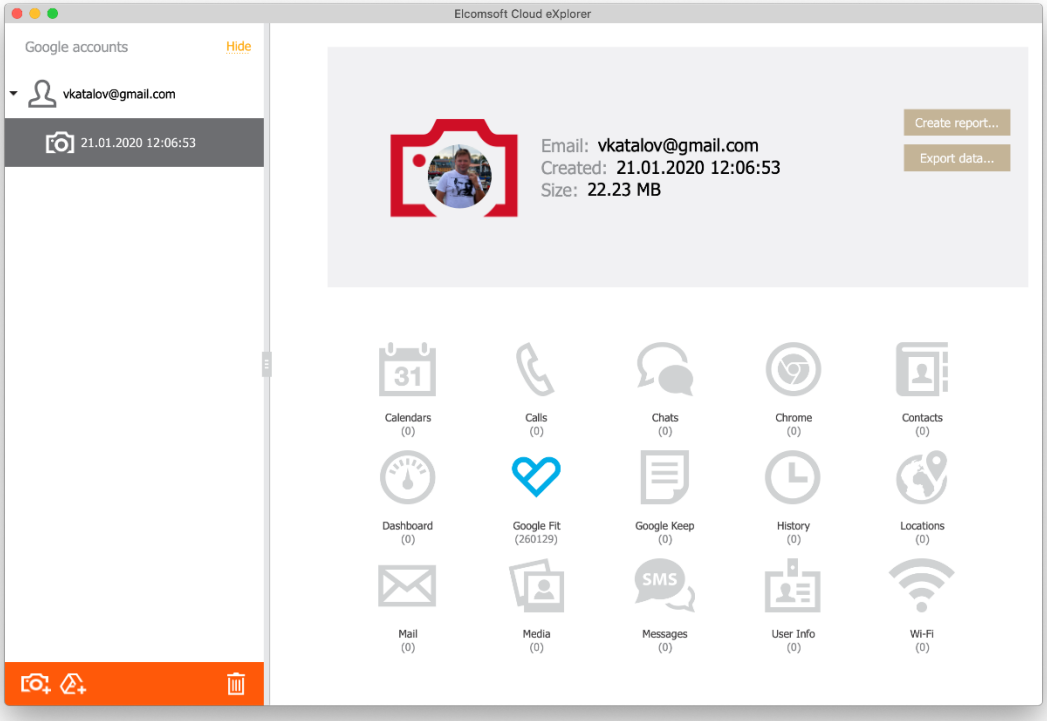
Security of health data in the cloud

- **Apple Health**
  - iOS 12 and 13 protect Health data with the user's device passcode
  - To extract, need all of the following: Apple ID, password, 2FA code, device screen lock passcode
  - Cannot be extracted from the cloud via GDPR requests; not provided to LE
- **Google Fit**
  - Stored in the cloud with no additional protection
  - Can be easily exported, extracted or requested from Google by LE

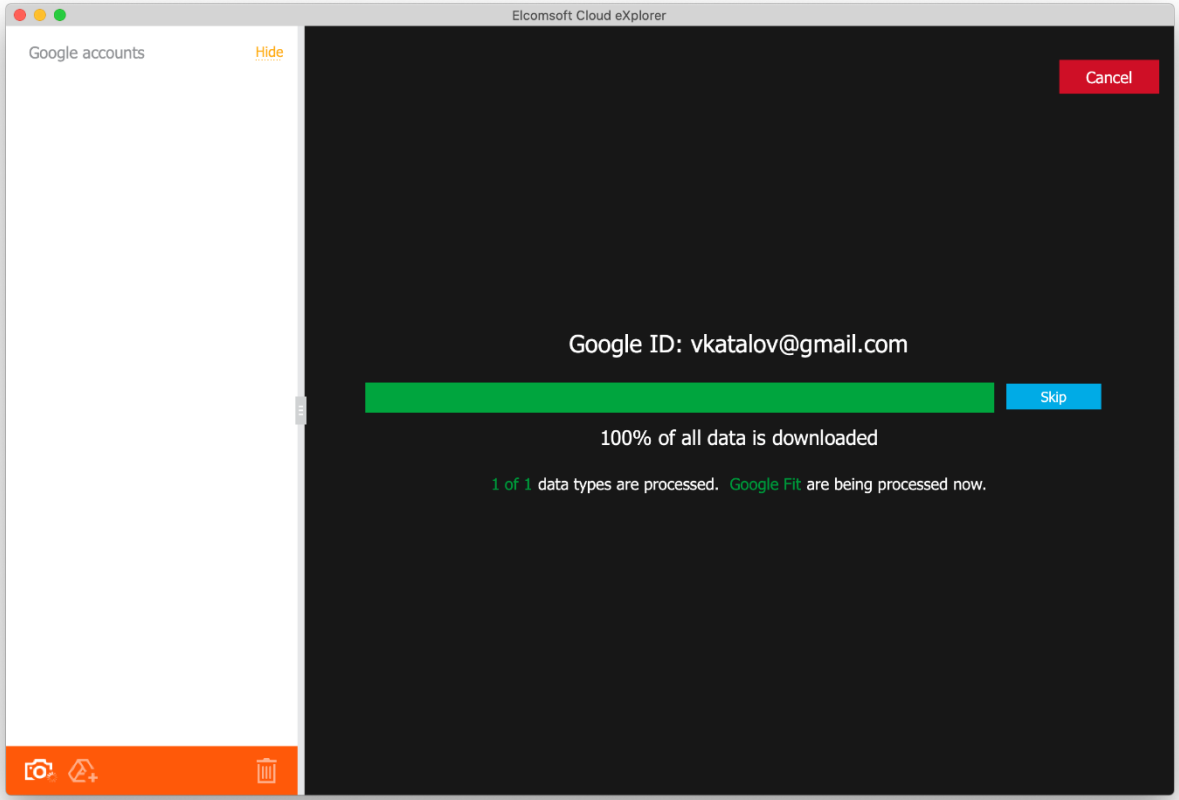
Google Fit Extraction

Google Fit data is stored in the Google Account

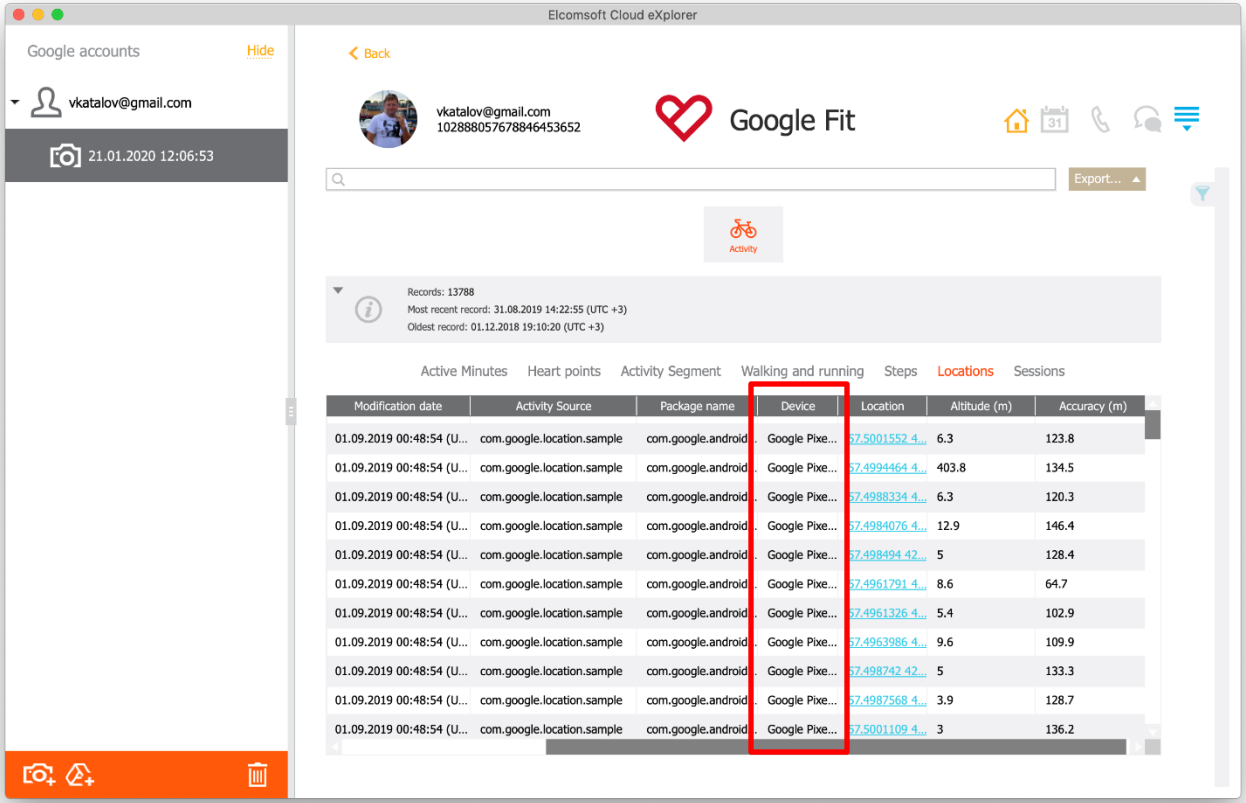
- Sign in using Google Account credentials
- Login, password and one-time code
- Note: Google Fit data has **no** point-to-point encryption



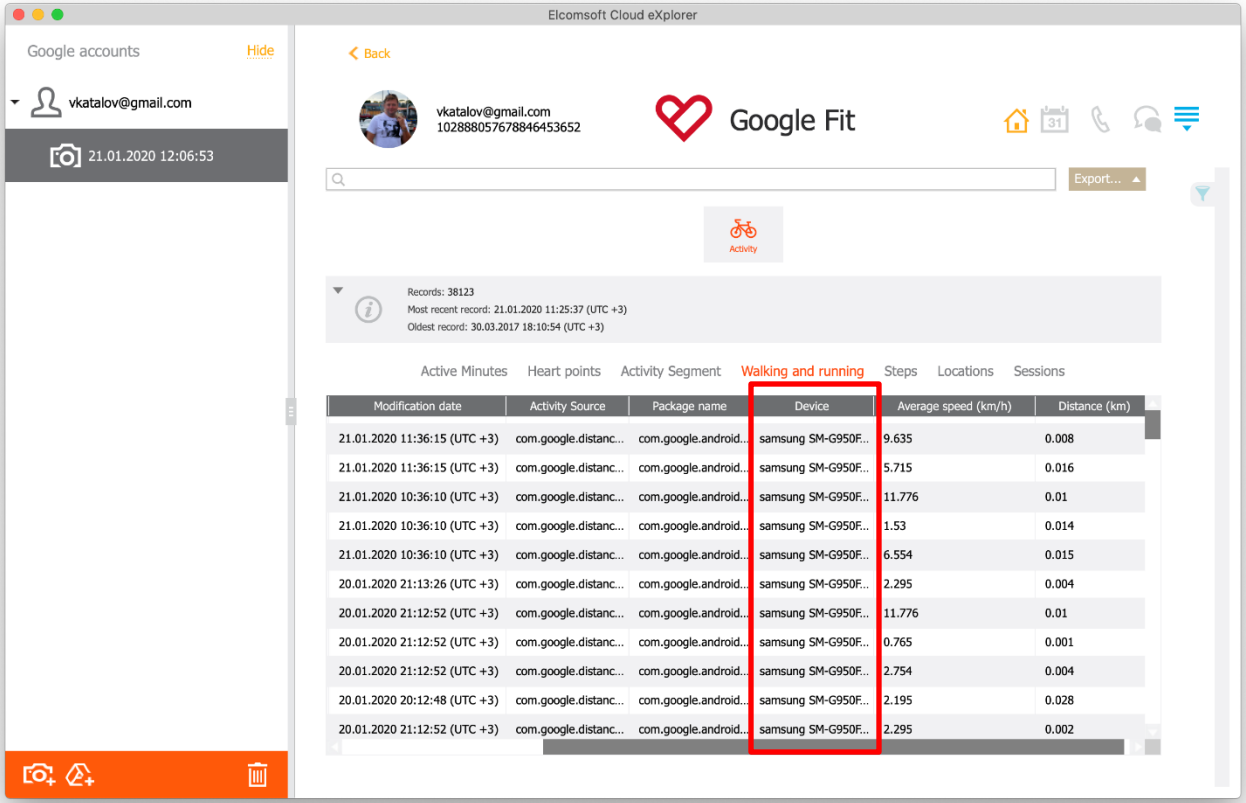
Google Fit Data



Google Fit Data



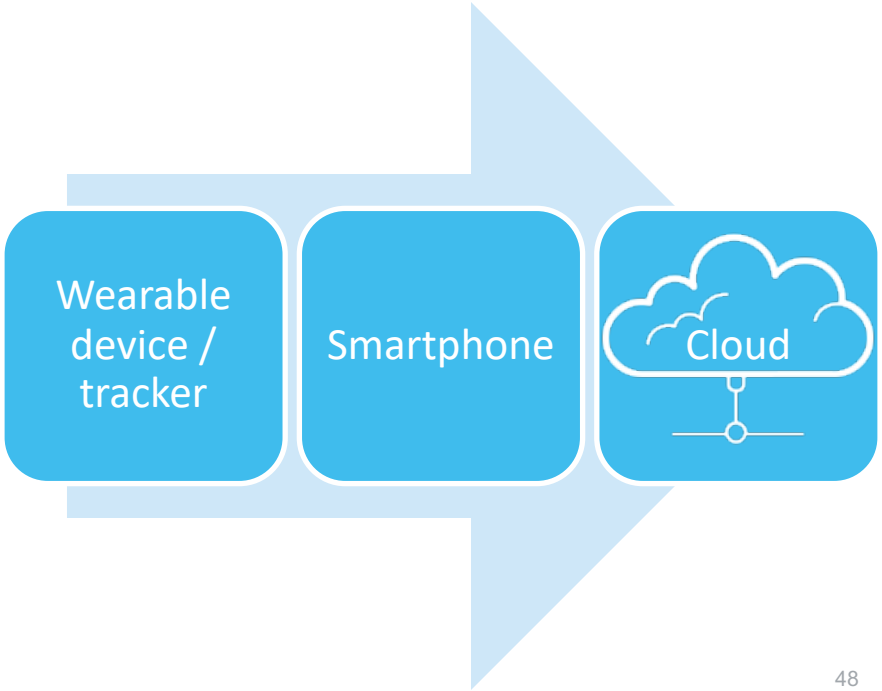
Google Fit Data



Wearables Data Flow

Wearable device > Phone > Cloud

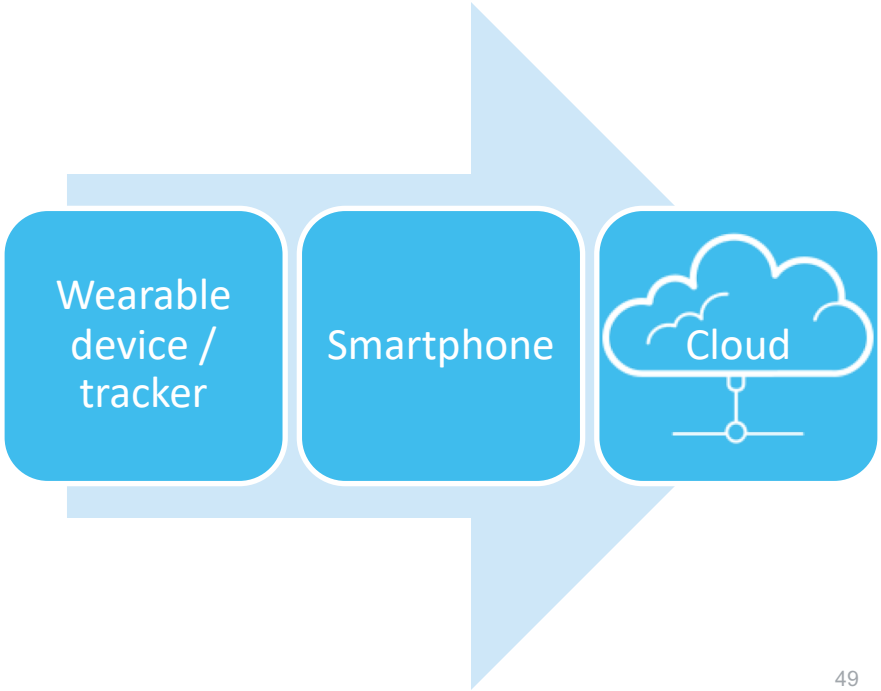
- The wearable device collects information (steps, heart rate, GPS, activity, screen time etc.)
- The data is synchronized with an app on the phone via a low-energy connection (e.g. Bluetooth LE, Wi-Fi and LTE sync available on some models)
- The app (Apple Health, Google Fit, Samsung Health, Mi Fit etc.) processes the data and (optionally) syncs with Apple Health Kit (or Google Fit on Android)
- And then…



Wearables Data Flow

Wearable device > Phone > Cloud

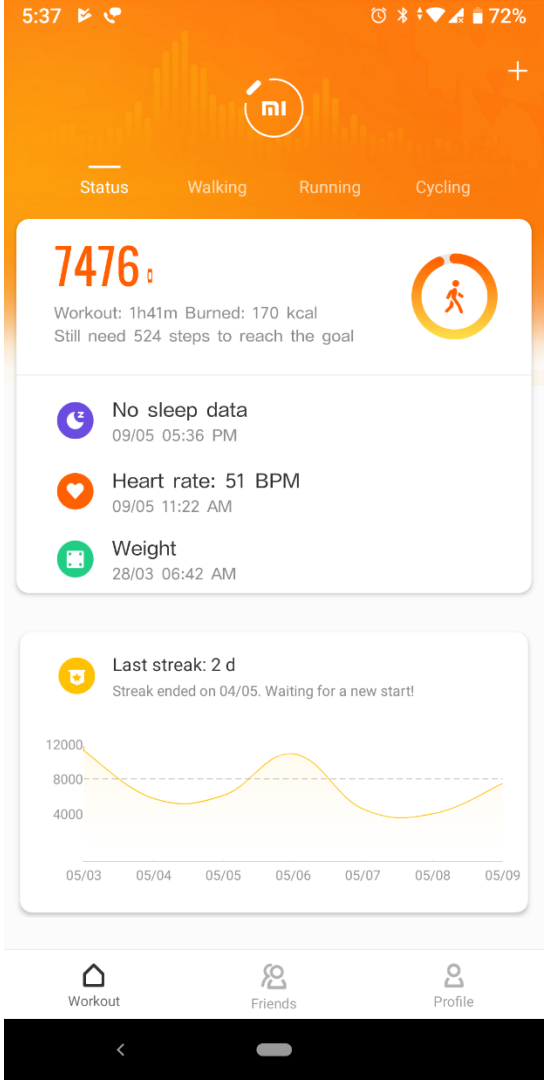
- The data ends up in the cloud
- If the data is synced with Apple HealthKit, the Health app aggregates the data and syncs with iCloud
- If the data is synced with Google Fit, then Google takes care of the sync
- More often than not, manufacturers employ their very own, proprietary cloud service
- **Such as Fitbit**



Data collected by vendors

Mi Fit

Data	Description
User profile	Information provided by the user such as age, height and weight
Device list	List of devices registered for Mi Fit
Running history	Detailed information about running workouts
Band data	Service information from the tracker device
Hearth rate	Raw hearth rate data
Event reminders	Events and reminders
Manual data	Any information the user added manually
Health settings	Settings of the Health app
ETE and THA events	ETE and THA rhythm events
Weight records	Timestamped weighing data



Data collected by vendors

Samsung Health

- As one can expect, Samsung collects lots of finely detailed information
- More than 100 distinct data categories
- As an example, ALP, albumin, amylase, blood pressure, blood glucose, caffeine intake, creatinine, CPK and bilirubin data fields are available for the blood
- Unsurprisingly, Samsung does not sync with Apple HealthKit or Google Fit, which define a much smaller (and less detailed) subset of health data

Data collected by vendors

Fitbit

- Fitbit collects, stores and processes data to estimate a variety of metrics
- The data is stored in Fitbit cloud
  - Step count and distance traveled
  - Calories burned
  - Weight
  - Heart rate
  - Sleep stages and active minutes
  - Location

Data collected by vendors

Where Fitbit stores data

- Fitbit stores data in the proprietary cloud service
- Fitbit offers a Web API to access data: https://dev.fitbit.com/build/reference/web-api/
- Web API gives access to all of the following:
  - Activity
  - Body & weight
  - Devices and alarms
  - Food logging
  - Friends
  - Heart rate
  - Sleep
  - User profile

Data collected by vendors

Data in Fitbit cloud

- **Activity**
  - **Daily activity summary** including:
  - **Daily goals for elevation (elevation, floors), steps, calories burned, and distance**
  - **Activity time series:** time series data in the specified range
  - **Activity logging:** the same data in user's local language
  - **Activity types:** a tree of all valid Fitbit public activities as well as private custom activities the user created
  - **Activity goals:** a user's current daily or weekly activity goals
  - **Lifetime stats:** the user's activity statistics

Data collected by vendors

Data in Fitbit cloud

- **Body & Weight**
  - **Body fat:** the list of all user's **body fat log entries** for a given day
  - **Body time series:** time series data in the specified range
  - **Goals:** a user's current body fat percentage or weight goal
  - **Weight:** a list of all user's body weight log entries for a given day

Data collected by vendors

Data in Fitbit cloud

- **Devices and alarms**
  - Data provided through the Fitbit API does not necessarily represent a single tracker
  - Data can change frequently, as trackers sync at different intervals and the unified data is recalculated at each sync
  - Distance and number of steps are correlated when GPS data is available

Data collected by vendors

Data in Fitbit cloud

- **Food logging**
  - Public and private food logs
  - Nutrition information
  - Hydration logs
  - Including goals and time series

Data collected by vendors

Data in Fitbit cloud

- **Friends**
  - List of user's friends
  - Links to friends profiles
  - Friends data (e.g. number of steps)
  - Invitations
  - Invitation responses

Data collected by vendors

Data in Fitbit cloud

- **Sleep logs**
  - Detailed information on the user's sleeping sessions
  - Sleep and awake minutes, time in bed, minutes to fall asleep
  - **Summaries**: minutes after wakeup, minutes asleep, minutes awake, minutes to fall asleep, start time, time in bed, sleep phase
  - Sleep phase ("level"): wake, rem, awake, restless, asleep etc.

Data collected by vendors

Data in Fitbit cloud

- **User profile**
  - Detailed information on authenticated user
  - Basic information about user's friends
  - No access to other users profiles

Fitbit Acquisition

Will Google acquisition of Fitbit affect the cloud?

- Most definitely, it will
- Fitbit acquisition gives Google access to a trove of data from sleep tracking to heart rates
- “Fitbit and Google Announce Collaboration to Accelerate Innovation in Digital Health and Wearables”
- “Fitbit to leverage Google Cloud to increase operational efficiency, agility and speed to mark
- “Fitbit intends to use Google’s new Cloud Healt API to help the company integrate further into t healthcare system”
- Source: Fitbit press release

Fitbit Acquisition

Does Fitbit acquisition affect users and/or forensics?

- No, at least not immediately
- The changes, if any, will occur slowly
- Most probably to new products only
- Most probably not before Q3’ 2020 anyway because of development pipeline
- Existing products will be likely grandfathered, keep using existing Fitbit services

January 2020

Health and Activity Evidence

How smartphones and trackers collect and store health data, and how to obtain health information

Vladimir Katalov, ElcomSoft