

The Wearipedia Project: a free and open-source resource for understanding and using wearables in decentralized clinical trials

Alexander Johansen*, Kyu Hur*, Jack Hung, Rodrigo Castellon, Tristan Peng, Stephanie Ren, Renee White,
Chanyeong Park, Allison Lau, Saarth Shah, Hee Jung Choi, William Wang, Pann Sripitak, Mohamed Elhusinni,
Michael Snyder

5

Department of Genetics, Stanford University, CA, USA

Summary

Background Finding the optimal wearable biomedical sensor (ref. wearable) for a clinical research study can be challenging. Many wearables are consumer electronics and are not designed for clinical research and their clinical variables vary widely. We aimed to build a resource for clinical researchers to select the best device for their research study, and programming tools to facilitate wearable research.

Methods For each wearable entry, we document the following— Open-source coding tools: we built data extraction, simulation, statistical testing, and educational materials; Clinical trial usage: trials using the device including ChatGPT-generated summaries; Privacy evaluation: low data risk, HIPAA compliance, de-identification, third-party data sharing, and third-party data sharing transparency; Security evaluation: wearable connectivity and API access protocols.

Findings The Wearipedia database consists of 19 wearables + 5 Apps; 7 smart watches, 4 fitness trackers, 2 chest straps, 2 CGM devices, 1 smart ring, 1 arm strap, 1 under the bed sleep tracker, 1 smart scale, 2 apps for diet tracking, 1 app for questionnaires, and 2 apps for data storage. For public coding tools, there were 891 pages of educational material across 22 wearables and apps. We support data extraction from 13 official APIs and 3 unofficial APIs under the Wearipedia pypi package. For clinical usage, there were 63 (± 99) clinical trials per device. For security and privacy, a total of 87 citations and an average of 3.48 citations are referenced, mostly consisting of privacy policies, terms-of-service agreements, and wearable manuals. The Wearipedia database is conveniently accessible through a website at <https://wearipedia.com>.

Interpretations Wearables can accurately predict important physiological parameters, glucose, and sleep. However, access to high resolution data can be restrictive, characterizing data accuracy is difficult, and wearable data is often not protected from third party reselling, including government requests.

Funding This work was made possible by the support of the BV and Anu Jagadeesh Family Foundation.

Keywords: wearables, clinical trial, accuracy, privacy, security

2000 MSC: [2010] 00-01, 99-00

*Corresponding author
Email: arjo@stanford.edu
URL: <https://wearipedia.com>

30 Introduction

Wearable biomedical sensors (i.e. wearables) are a group of electronic devices that can provide continuous, inexpensive, and real-time physiological information using either noninvasive or minimally invasive measurements¹. Although not generally FDA approved for most applications, individuals, clinicians, and clinical researchers can use wearable sensors to track patient health data and conduct decentralized clinical studies and trials^{2,3}. In decentralized clinical studies, the clinical researcher might not have direct contact with the test subject and requires remote collection of health parameters. Wearables provide decentralized clinical studies with a tool that is inexpensive (as low as US\$80 per subject), allows 24/7 monitoring, only requires partial internet connectivity, and are designed to be minimally intrusive to the users daily tasks^{4,5}. Recent efforts in clinical studies have shown promising results using wearables to predict features such as COVID-19 before symptom onset^{6,7}, menstrual cycle and pregnancy^{8–10}, and abnormal heart function¹¹. These advances come through developments in modern sensor technology and signal processing that takes raw sensor output and produces meaningful high-level features through mathematical modeling that researchers can access through wearable manufacturer application interfaces (APIs) (ex. Oura, Fitbit) or software development kits (SDKs) (e.g. Health kit). Figure 1 provides a screenshot of a device in the Wearipedia database, namely the Oura Ring gen 3. The website contains detailed information on device capabilities and use, educational material, API tools, and concerns about privacy and security. The Wearipedia website covers the Oura Ring gen 3 and many other popular devices.

The wearable tech market, valued at US\$121.7 billion in 2021, is expected to surpass US\$392.4 billion by 2030, driven by major tech companies entering healthcare. Five companies (Apple, Fitbit, Samsung, Xiaomi, Huawei) dominate 60% of the market, restricting data access and complicating clinical research due to proprietary systems and limited APIs. Research-oriented wearables offer better support but are expensive and less reliable. Moreover, there's constant change with vendors abruptly discontinuing products and platforms.

The screenshot shows the Wearipedia website for the Oura Ring. At the top, there are tabs for Wearipedia, Wearables, Tutorials, About Us, User Agreement, Docs, and a search bar. Below the header, there are four tabs: SPO2 (selected), HR, 2-Stage, and Pedometer. To the right of these tabs is a Calorimeter icon. The main content area is divided into several sections:

- Overview of the Oura Ring:** A summary of the device's features, mentioning its validation for 2 stage sleep classification and 5 stage sleep detection, and its use in clinical trials. It highlights its ability to track heart rate, heart rate variability (HRV), and elevated body temperature, as well as physical activity and lifting.
- Daytime:** A table showing performance metrics for different activities:

Name	Performance	Frequency
HR	12.9	MAE
Pedometer-walk	52	daily (per min)
Pedometer-run	89	daily (per min)
- Nighttime:** A table showing performance metrics for sleep stages:

Name	Performance	Frequency
SPO2	3.2	MAE
HR	3.6	MAE
SOL	9.1	MAE
TST	19.97	MAE
WASO	3.4	MAE
SE	0.3	MAE
Stages	W/R	MAE
Apnea	N	MAE
Snoring	N	MAE
- Sensor Performance:** A table showing PPG and Pedometer data for the Oura Ring 3:

Series	PPG	Pedometer
Oura Ring 3	28.2 MAE	63 MAE
- Studies using Oura Ring:** A section listing clinical trials using the Oura Ring, with categories for Bariatrics, Cardiology, Chronic Pain Or Diseases, and Endocrinology. A "Show More" button is present.
- Privacy:** A section detailing privacy and data sharing concerns, including Data Risk (No), HIPAA Compliance (No), De-identification (Yes), Shares With Third Parties (No), Transparency in Third Party Sharing (No), Security (Wearable Connectivity Yes, API Access Security Yes), and a note about the trial's impact on quality of life.

```
import wearipedia
device = wearipedia.get_device("garmin/fenix_7s")
device.authenticate({"email": "foo@gmail.com", "password": "bar"})
data = device.get_data("steps")
```

Figure 1: **Top:** Webpage of wearable device - Oura ring. Top left is an overview summary of the clinical performance and usability. Bottom left is security and privacy concerns with detailed drop-out descriptions. Right is clinical performance with links to studies. Performance metrics are in standardized formats detailed in a performance metric section, and reviewed in the top-left overview summary. Bottom right are clinical-trials.gov studies that utilizes the wearable with autogenerated summaries by ChatGPT. **Bottom:** Code snippet demonstrating data extraction for the Garmin Fenix 7S device. It's only four lines.

We developed the Wearipedia, which is a comprehensive database covering 19 wearable devices and 5 apps in order to provide easy access for clinicians and researchers to downloading wearable data. Critically, it addresses privacy, 85 usability, and data extraction challenges. The platform includes extensive Python resources, aiming to assist clinical researchers in selecting and using wearables effectively. Unlike existing databases, Wearipedia offers in-depth analysis and novel simulation tools—filling a gap in pre-clinical and operational wearable research. The database is open-source and continuously updated, providing valuable resources for both novice and experienced researchers and requires only basic Python programming skills. Specifically, our Python package, also called `wearipedia`, streamlines 90 the process of extracting data from wearable device APIs. With just four lines of code, anyone is able to extract data from any wearable device included in our package, as seen in Figure 1.

Research in context

Evidence before this study

The Wearipedia ties together many novel topics into one database, including: privacy, security, data extraction, open source, educational material, clinical trial tracking. As the purpose of the Wearipedia is to tie together these resources to compare with public websites and databases.

Website and database: We performed a Pubmed search for ("wearable" OR "wearables") AND ("clinical research" OR "clinical studies" OR "healthcare" OR "biomedical research") AND ("data studies" OR "healthcare" OR "biomedical research") AND ("data extraction" OR "data access" OR "data management") AND ("databases" OR "database")) with 25 hits and a Google search for: "Wearable databases" in which we investigated the first 20 hits, and asked OpenAI's GPT-4o for databases of wearables.

Our initial search revealed a patchwork of resources on wearable devices; databases like PhoneDB, GoHumanFirst, AtalasEDU, Vandrico, and DataverseNo¹² providing only basic details such as price, production year, and sensor types.

Added value of this study

Website and database: To our knowledge, this is the first study to provide an open-source unified comprehension of wearable devices. We scrutinized privacy & security issues while offering detailed, device-specific coding resources for data extraction and analysis. By integrating aforementioned resources, we provide a holistic overview of each device in just one page. This sets a new standard for how researchers interact with wearable technology.

Implications of all the available evidence

Navigating the complexities of wearable tech is no small feat. With Wearipedia, clinical researchers of all levels have a single, comprehensive hub that makes wearable device selection and use both straightforward and effective, accelerating advances in decentralized clinical studies.

Methods

To be adopted in the Wearipedia database and displayed on the website a host of content have to be covered in detail 95 guiding users from search phase through deployment; Base requirements, API access & Wearipedia python package, Educational Material, Clinical Trial Tracking, and Privacy & Security.

Basic device or app requirements

The mission is to empower clinical researchers performing decentralized clinical studies and trials with minimal participant burden. Consequently, the device/app must be wearable or usable at-home. It must be non-invasive, which 100 for now excludes at-home blood testing. No in-clinic visits should be necessary. It must be related to some type of physiology measurement. A device must be purchasable at minimum in the US or EU, either publicly or through medical offices for patient treatment (i.e. certain continuous glucose monitoring (CGM) or heart monitoring devices).

API access & Wearipedia python package

At the Wearipedia project, we commit to empowering clinical researchers by fully open-sourcing all device connectors. Therefore, any device included MUST have API access to device data. Devices without API access are excluded. Partial data is accepted (e.g. most devices give device summaries only). The device must be submitted to the open-source 105

Wearipedia Python Package. In particular, we require that reasonable functionality is present and data simulators are built for allowing researchers with limited device access the ability to test devices before purchasing them. Moreover, simulated data is necessary for developed educational content. Devices will be reviewed on a device-by-device basis. Details on device submission processes can be found in Appendix A.

Educational Material

To strengthen the clinical research community, we developed significant educational resources for clinical researchers with limited exposure to programming and data analysis. In particular, we want to guide clinical researchers through the basics of conducting and evaluating data from wearable devices. Our format of choice is Jupyter Notebooks in the Python coding language. For each educational notebook, we require the following steps for a notebook covering a single wearable with a single participant and a single study coordinator.

1. A 1-page letter detailing setup for the user, and a formal guide of what is expected of the user in the remainder of the clinical study.
2. A setup guide for the clinical researcher to ensure access to data for one user.
3. Data extraction using the Wearipedia python package for one user.
4. Data simulation using the Wearipedia python package
5. Guide on how to port data to R, Matlab, Excel, and standard data formats using the Wearipedia python package.
6. Minimum 2 plots visualizing details of wearable data
7. Guide, and visualization, on how to remove non-adherence for a custom period and custom adherence percentage (e.g. days, weeks, months).
8. Guide, and visualization, on how to remove outliers using statistical testing.
9. Guide, and visualization, on how to test a hypothesis.

The notebook must be subsequently submitted to the repository, and accepted through internal code-review ensuring it meets strict educational standards.

Clinical Trial Tracking

Any device must have automatically updated summaries from the newest data available about the device on clinicaltrials.gov. In particular, we utilize the CliniDigest¹³ tool that scrapes, filters, and classifies clinical trials for wearable devices across 14 medical categories. Setting up CliniDigest for a new device is easy and simply requires defining useful keywords that sufficiently capture the clinical trials of choice. Details on what keywords to use, examples of other devices, and formal requirements for making a pull request is available at <https://github.com/Stanford-Health/CliniDigest>. The CliniDigest tool is automatically run every Sunday and updates summaries if new trials are available.

Privacy & Security Device Evaluation

Privacy and security safeguards grow ever more urgent as digital systems erode individual control over personal data. While scholars still debate an exact definition of privacy^{14–19}, most agree privacy underpins autonomy and liberty and thus warrants strong regulation²⁰. Additionally, consentless sharing of data, real-time tracking of sensitive information, ambiguous terms of services, and weak authentication or encryption protocols are widespread^{21–24}. The World Economic Forum lists data fraud and cyber attacks among the five likeliest global threats this decade²⁵, and wearable ecosystems supply fertile ground—limited processing power, small batteries, unsecured Bluetooth, and rushed design cycles^{26–29}. Lax developer practices³⁰ and documented hacks³¹ have already exposed user data. Roughly one-third of U.S. adults already use a wearable device^{32–34} with sensors that record highly confidential health metrics^{35,36}, yet are unregulated by the Food and Drug Administration and is beyond comprehensive laws such as HIPAA^{37–39}. API-centric architectures enlarge the attack surface—public endpoints and microservices enable scraping or credential-stuffing, while insecure companion apps spread vulnerabilities from wrist to network^{40–43}.

Scholars therefore urge a dedicated, binding privacy standard for health-monitoring wearables. In particular, we designed a set of relevant metrics to rate the privacy and security of wearable devices, documented in full in Appendix D. The privacy and security rating of each wearable device is measured under seven different criteria (5 under Privacy, 2 under Security) in Table 1.

Metric Category	Rating	Brief Description
Privacy	Low data risk	Wearable collects potentially sensitive information
Privacy	HIPAA compliant	Company does not collect personally identifiable information defined under HIPAA
Privacy	De-identification when sharing	Company de-identifies data when publicizing or sharing with other entities
Privacy	No third party sharing	Company commits to not sharing with third-parties
Privacy	Transparency in third party sharing	Company is exhaustively transparent with which entities data may be shared to
Security	Secure wearable connectivity	Wearable utilizes WiFi to connect to persistent stores
Security	Secure API access	Wearable provides API access through OAuth 2.0 protocol

Table 1: Brief descriptions of all seven privacy and security rating metrics. 5 ratings are under privacy, with 2 others under security. Longer, in-depth descriptions of each rating is provided in Appendix D.

155 Wearipedia Website and Database

We recognize that the information presented in the Wearipedia database can be overwhelming. Wearable biomedical sensors have significantly changed the landscape of clinical research and the requirements for clinical researchers. In particular, with understanding minute details on complex electrical devices and convoluted coding projects. To ease the process from start to finish we have adopted modern user-experience practices in designing a website for searching through Wearipedia entries and visualizing an entry on a single simple and intuitive page. The website was developed in Javascript with MongoDB, Express.js, and Node.js, then hosted on AWS. Each Wearipedia database entry is stored as a JSON entry. The raw Wearipedia JSON entries are open-source. The website design and layout is kept private due to security concerns.

Results

- 165 Following the requirements outlined in the methodology section, we have the following as per April 2025: 19 Wearables and 5 Apps; 7 smart watches; 4 fitness trackers; 1 chest straps; 2 CGM devices; 1 smart ring; 1 arm strap; 1 under the bed sleep tracker; 1 smart scale; 2 apps for diet tracking; 1 app for questionnaires; and 1 apps for data storage.

API access & Wearipedia python package

In Table 2, we cover API type, sampling rates, data simulators, and API-related concerns along with required permissions. The sampling and concerns are of particular importance as while a device might potentially have the capability to empower certain studies, poor sampling or data access can make it infeasible in practice. Notably, Whoop strap only has daily summaries, Garmin Fenix uses Oauth 1.0 which is insecure, Oura ring and Fitbit requires team approval for full data access, and Apple Watch does not have a public API, but requires developing and proceeding an app for data access. Interestingly, apps such as EliteHRV have developed a niche product to interface with Polar for high resolution, beat-to-beat data.

API Type	Sampling	Simulator	Concerns
<i>Fitness Trackers</i>			
Oura Ring	OAuth 2.0 HR: 5 min Steps: Daily Sleep stages: Daily Temperature: Daily *Interbeats: Full *Hypnogram: 30 sec	HR, Steps, Sleep	Requires Oura team's authorization for full data access, only sleep data is reliable. 30 days can be requested at a time without contacting Oura.

Continued on next page

Continued from previous page

	API Type	Sampling	Simulator	Concerns
Polar Vantage	OAuth 2.0	HR: 5 min Steps: Daily Sleep Stages: Daily	HR, Steps, Sleep	Only allows pulling data from the last 30 days. Can only pull data from dates occurring after the user has authorized the app, so this must be done at the beginning of the study.
Fitbit Sense, Charge, Versa	OAuth 2.0	HR: 1 min Steps: Daily HRV: per sleep SpO ₂ : 5 min Sleep Stages: Daily	HR, Steps, HRV, Sleep	API rate limits at 150 requests per hour per user, and intraday data requires one request per day.
Garmin Fenix	OAuth 1.0	HR: 2 min Sleep Stages: Daily Steps: 15 min SpO ₂ : Daily HRV: Daily	HR, Sleep stages, Steps, HRV	Integrated APIs are using unofficial libraries and may not have guaranteed stability; these libraries are well-supported historically.
Whoop Strap	OAuth 2.0	HR: Average per day HRV: Average per day SpO ₂ : Average per day Sleep: Daily	HR, HRV, SpO ₂	Calculated sleep and recovery scores are available, but underlying data measurements are not queryable.
Withings ScanWatch	OAuth 2.0	HR: 10 min, higher during workout mode Sleep: Daily Sleep Stages: Daily ECG: On demand	HR, Sleep	Also provides a raw data mode which provides access to high-frequency PPG and accelerometer data
Biostrap	OAuth 2.0	Workout (Activities): per session HR: 10 min Breaths per Minute: 1 min HRV: 10 secs SpO ₂ : 10 secs Resting Calories: Daily Workout Calories: Daily Active Calories: Daily Step Calories: Daily Total Calories: Daily Sleep Movements: per session Sleep Biometrics Details: per session Steps: 1 min Distance: 1 min	Activities, HR, BRPM, HRV, SpO ₂ , Resting Calories, Workout Calories, Active Calories, Step Calories, Total Calories, Sleep Movements, Sleep Biometrics Details, Steps, Distance	Requires a form submission for access to the API

Continued on next page

Continued from previous page

	API Type	Sampling	Simulator	Concerns
Coros Pace	No auth flow; access token from browser	Steps: 30 minutes HR: 30 min SpO ₂ : 30 min	Steps, HR, SpO ₂	No public developer API; access requires submitting an application to COROS. Research applications are deprioritized and are unlikely to get a response.
Apple Watch	SDK	N/A	N/A	Can be accessed only through SDK meaning that an app has to be developed and accepted in the Apple store to gain access.
<i>Heart Rate Monitoring Belts</i>				
Polar H10	OAuth 2.0	HR: Second (polar API) RR: Millisecond (EliteHRV)	HR, HRV	Only allows pulling data from the last 30 days. Can only pull data from dates occurring after the user has authorized the app, so this must be done at the beginning of the study. Must record activity for measurements through app. Must use EliteHRV for higher quality data.
Polar Verity Sense	OAuth 2.0	HR: 5 min	HR	See Polar H10
<i>Accelerometers</i>				
Actigraph CentrePoint Insight	OAuth 2.0	Activity Intensity: 1 day MVPA: 1 day Steps: 1 day Calories: 1 min Activity Counts: 1 min Sleep Status: 1 min	Activity Counts, MVPA, Sleep Status	To access all data, must not be using demo study program.
<i>Continuous Glucose Monitoring Devices</i>				
Dexcom Pro CGM	OAuth 2.0	Blood Glucose: 5 min	Blood Glucose	Requires an application to get access to any production data. Access to personal data can be granted within a few days, while research applications might take 8-10 weeks.
Abbott Freestyle Libre	OAuth 2.0	Blood Glucose: 15 min	Blood Glucose	Does not provide an API, requires the use of a third-party integration
<i>Data Gathering Apps</i>				

Continued on next page

Continued from previous page

	API Type	Sampling	Simulator	Concerns
Apple HealthKit	SDK	N/A	N/A	Access only through SDK meaning that an app has to be developed and accepted in the apple store to gain access.
Strava	OAuth 2.0	Activity Data: per run HR: Continuous while activity is being recorded and a compatible fitness tracker is being used	Activity data, HR	Data is either manually recorded or automatically using a fitness tracker, so the granularity and accuracy of data depend on the method of collection.
EliteHRV (with data collected by Polar H10)	Username and Password	RR intervals: Milliseconds (can derive HRV, HR)	RR	Only allows pulling data from the last 30 days. Can only pull data from dates occurring after the user has authorized the app, so this must be done at the beginning of the study.
<i>Smart Phones</i>				
Apple iPhone	SDK	N/A	N/A	Access only through SDK meaning that an app has to be developed and accepted in the apple store to gain access.
<i>Sleep Mats</i>				
Withings Sleep	OAuth 2.0	Sleep: Daily HR: While sleeping, every 10 min	Sleep, HR	N/A
<i>Smart Scales</i>				
Withings Body+	OAuth 2.0	Weight Data: per use	Weight, Fat ratio	N/A
<i>Calorie Trackers</i>				
Cronometer	Basic Authentication	Daily summary Nutrition data Exercise data Biometric data	N/A	All data is manually recorded
MyFitnessPal	Cookie-based Authentication	Goals data Daily summary Exercise data Meal data	N/A	All data is manually recorded
<i>Questionnaires</i>				

Qualtrics	Token-based Authentication	Pandas DataFrame of all questions and answers for a given survey, along with basic survey metadata fields	CSV file of a sample patient intake questionnaire is included (instead of simulator)	Integrated APIs are using unofficial libraries and may not have guaranteed stability; historically these libraries are well-supported.
-----------	----------------------------	---	--	--

Table 2: Information on API type, sampling details, simulator, and potential concerns for each wearable device sectioned by fitness trackers, HR belts, accelerometers, CGM devices, data gathering apps, smart phones, sleep mats, smart scales, calorie trackers, and questionnaires.

*: includes special deals with the wearable vendor such as Fitbit Intraday and Oura Labs

Educational Material

A major contribution of the Wearipedia is helping clinical researchers adopt python and guide data extraction, visualization, and analysis pipelines. Through detailed python notebooks, broken into 9 topics as covered in Figure ??, we provide more than 15,000 lines of code and text description.

Section Distribution across 19 notebooks totalling 15011 lines of content

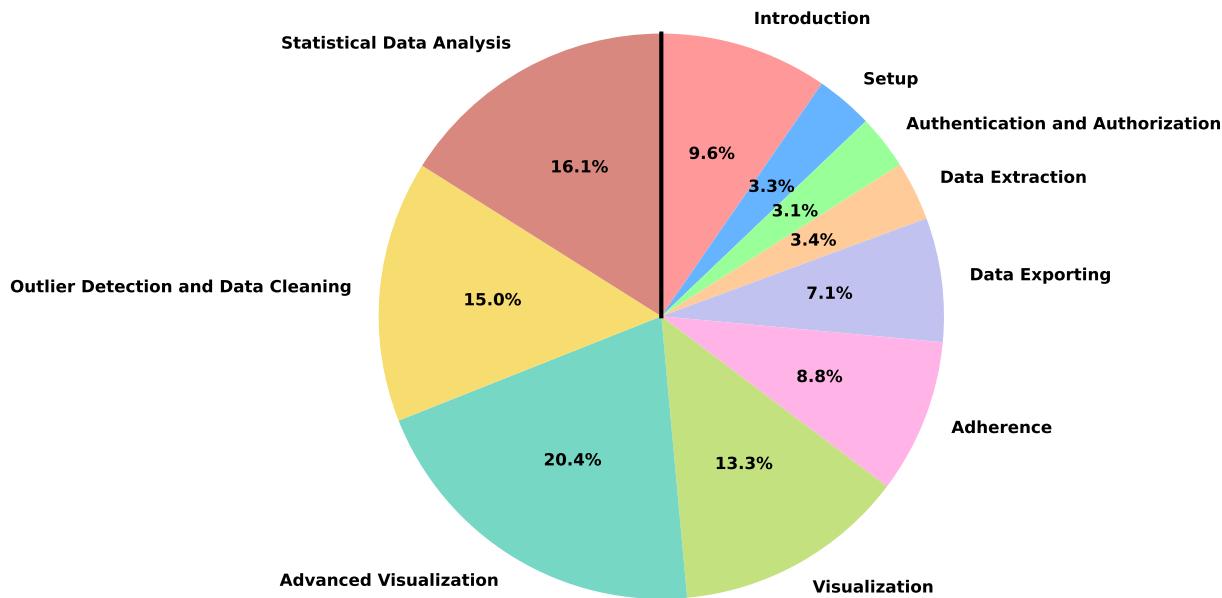


Figure 2: **Notebook content distribution**—the Wearipedia contains 21 notebooks: 19 single-participant data flow and 2 multi-participant data flows. This figure highlights the distribution of educational material over the 10 single-participant notebooks totaling 15,000 lines of code and text descriptions. Noticeable is that more than half of the content is catered towards more advanced data modeling (Advanced Visualization, Outlier Detection & Data Cleaning, and Statistical Data Analysis). This highlights a highly developed resource for clinical researchers to get started on their wearable data analysis journey.

180 Clinical Trial Tracking

A clear understanding of previously conducted research is paramount to choosing the best device and planning a new clinical trial. CliniDigest provides summaries of clinical trials involving wearable devices within 14 different fields of medical specializations. Updated automatically weekly through data extraction from ClinicalTrials.gov, CliniDigest produces and publishes new summaries encapsulating the current state of research using wearable devices. The pipeline includes papers up to five years old and a list of regular expressions encapsulating the search terms defined in Appendix C. A wide range of wearable devices are used in clinical trials, as depicted in Figure 3. Devices such as Abbott Freestyle Libre and Dexcom G Pro are primarily used for one medical field. In contrast, other devices, such

as the iPhone and Fitbit devices, are used across several medical fields. As designed, as the number of clinical trials being summarized in a given summary increases, the summary becomes more general, citing fewer trials while still encompassing the trends and uses of the given wearable device. For example, 120 clinical trials address endocrinology using the Abbot Freestyle Libre system, with only four specifically cited to provide concrete examples in the summary below.

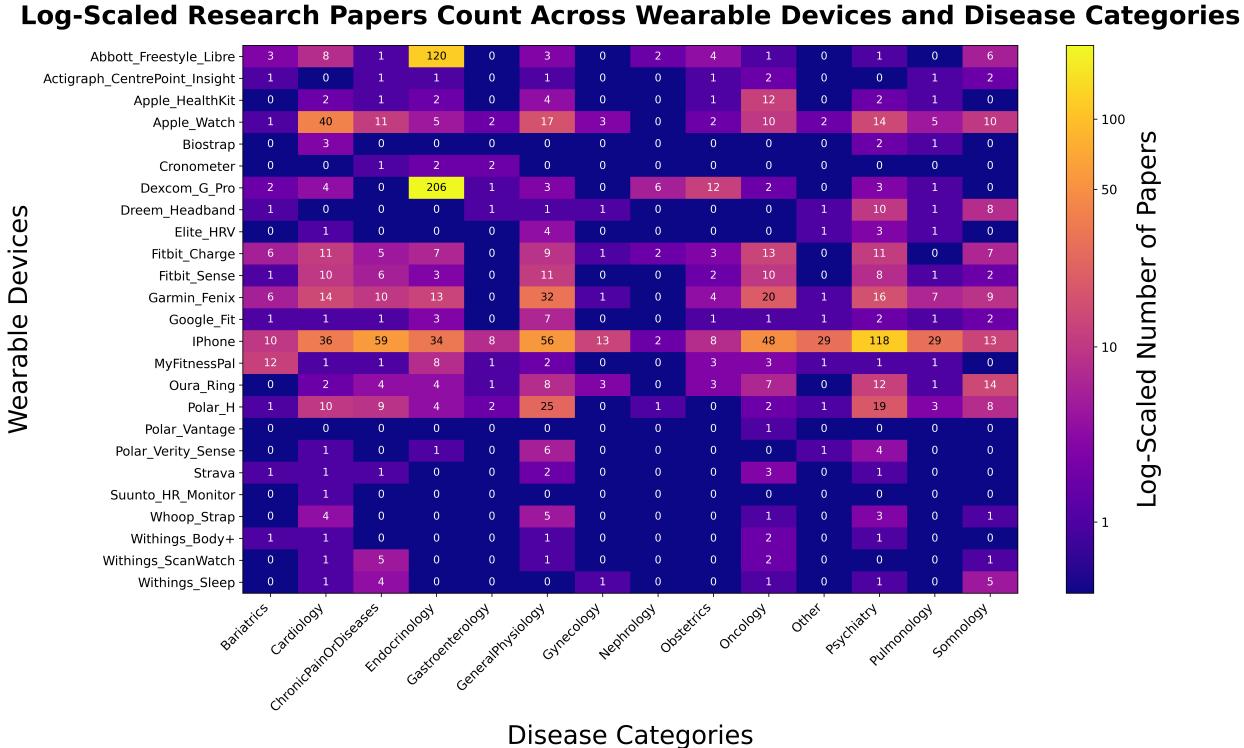


Figure 3: **Clinical Trial count**—y-axis is wearable device and x-axis is medical field. Each cube corresponds to the number of clinical trials on clinicaltrials.org that CliniDigest has found through its search criteria. These Clinical Trials are then included in a 200 word summary placed on each wearable device page on the Wearipedia website.

Privacy & Security Device Evaluation

Each wearable was evaluated separately, but many had overlapping sources and gray literature that often resulted in identical scores. A full list of wearable devices are available in Table 3, denoted by company and model name. All wearables failed low data risk. By nature of the data collected, all wearables collected some data that could be categorized as a risk to privacy—either through primary or predictive data. All failed to be HIPAA compliant, as all vendors enforced some mechanism to collect personally identifiable information (PII) from users. This is most common in the form of name and e-mail address, though quite a few other vendors collected other PII. No company offered full access to their wearable device without requiring users to relinquish PII. Some wearable devices included a clause within their privacy policy or terms of service about de-identifying the data when sharing with other parties. Those that did not include this clause were Abbott Libre 2, Actigraph CPI, Coros Pace 2, Dexcom Pro CGM, Fitbit Sense/Charge 4, Garmin Fenix 7S, Nutrisense CGM Patch, Oura Ring 3, Polar H10/Vantage 2/Verity Sense, SleepOn go2sleep, Suunto HR Monitor, and Withings Body+/ScanWatch/Sleep. It may be the case that these wearables de-identify their data when sharing with other parties, but there was no explicit mention within their terms of use or privacy policies. All wearables included a clause about sharing data with third parties. This was most commonly stated in the privacy policy or terms of use. Similarly, all but one did not exhaustively disclose the list of third parties that they may share data with. Most wearables stated some variation of "other", "miscellaneous", or "various" third parties that may currently or at a different time point gain access to user data. Only Garmin exhaustively listed the third parties that will gain access to user data.

Company	Model Name	Low Data Risk	Compliant with HIPAA	De-identifies Data When Sharing	No Third Party Sharing	Transparency in Third Party Sharing	Secure Wearable Connectivity	Secure API Access
Abbott	Libre 2	✗	✗	✗	✗	✗	✓	—
Actigraph	CPI	✗	✗	✗	✗	✗	✗	✓
Apple	Health kit	✗	✗	✓	✗	✗	—	✓
Apple	Watch 5	✗	✗	✓	✗	✗	✓	✓
Apple	Watch Ultra	✗	✗	✓	✗	✗	✓	✓
Apple	iPhone	✗	✗	✓	✗	✗	✓	—
Coros	Pace 2	✗	✗	✗	✗	✗	✗	—
Dexcom	Pro CGM	✗	✗	✗	✗	✗	✗	✓
Fitbit	Sense	✗	✗	✗	✗	✗	✓	✓
Fitbit	Charge 4	✗	✗	✗	✗	✗	✓	✓
Garmin	Fenix 7S	✗	✗	✗	✗	✓	✓	✗
Nutrisense	CGM patch	✗	✗	✗	✗	✗	✓	—
Oura	Ring 3	✗	✗	✗	✗	✗	✓	✓
Polar	H10	✗	✗	✗	✗	✗	✓	✓
Polar	Vantage 2	✗	✗	✗	✗	✗	✗	✓
Polar	Verity Sense	✗	✗	✗	✗	✗	✓	✓
SleepOn	go2sleep	✗	✗	✗	✗	✗	✗	—
Suunto	HR Monitor	✗	✗	✗	✗	✗	✗	✓
Whoop	Strap 4.0	✗	✗	✓	✗	✗	✗	✓
Withings	Body+	✗	✗	✗	✗	✗	✓	✓
Withings	ScanWatch	✗	✗	✗	✗	✗	✗	✓
Withings	Sleep	✗	✗	✗	✗	✗	✓	✓
-	Cronometer	✗	✗	✓	✗	✗	—	—
-	MyFitnessPal	✗	✗	✓	✗	✗	—	✓
-	Strava	✗	✗	✓	✗	✗	—	✓

Table 3: Wearable devices and smartphone apps evaluated for privacy and security concerns across seven different categories. A green check mark signifies a satisfactory result defined by a specified threshold, whereas a red x mark means it is unsatisfactory. A dashed line indicates that result is not applicable (e.g. Apple health kit is not a wearable), so secure wearable connectivity cannot be described. Detailed descriptions of each metric as well as the threshold for satisfactory performance are detailed in Appendix D. Citations for how each rating was achieved is also provided in D.4.

Discussion

Most noticeable devices

Fitness: The Polar H10 is a chest strap that is considered the gold standard for many studies w.r.t. accurate heart rate and HRV measurements at only US\$105 (excluding taxes) and long battery life. However, an additional app, EliteHRV 215 is needed to extract data at US\$30-100 per month for a cohort. Moreover, a belt could lower user adherence compared to a ring or wrist strap.

Sleep: We find that the Oura ring is a great option for sleep study tracking due to great performance on sleep metrics, high quality data access, long battery life, and low concerns with user compliance due to the unobstructedness of wearing the device. However, the Oura ring is pricey (US\$349 excluding taxes), needs special access for high quality 220 data extraction, demonstrates low capabilities in step and physical activity detection, and potentially requires removal before manual labor or strength training—resulting in the loss of valuable data during such activities.

Budget friendly: The Fitbit Charge 6 costs only US\$160 (excluding taxes), has medium-to-high sleep and step prediction capability, battery life, high quality data access, can be used both while sleeping and for most physical activity.

Apple Watch: While achieving high performance across the board, the Apple Watch has concerns with battery life, 225 being uncomfortable while sleeping, a large screen that can interfere with study participants, and limited access to high quality data. For improved battery life Apple Ultra can be considered, but it comes at a hefty price point.

Interoperability between devices

Polar for fitness activities, Fitbit for step counts, Oura for sleep, Dexcom for CGM, and MyFitnessPal for diet tracking—should be simple? Unfortunately, no vendor has kept interoperability in mind and merging datasets as 230 well as timestamp is the clinical study coordinators' responsibility. The Wearipedia python package and the educational materials offer tools to ease the process (how to extract, find missing data, visualize, and perform statistical analysis). However, there is limited merging material.

Wearipedia website and Database

The Wearipedia project provides curated information about wearable devices to accelerate pre-clinical studies and 235 education of wearable devices. The website is easy to navigate and well documented. Currently 24 wearable devices and 5 apps are covered. The educational material is meant as an inspiration, and a starting point, for clinical researchers looking to work with wearable devices. Given all elements of the Wearipedia project is open source, future additions of wearable device and app pages from both in-house and external contributors is supported and encouraged. In the future we would like to extend to actively support clinical studies from start to finish.

What wearables devices to include next?

Popular fitness trackers: We have left out some key commercially, and cheap, wearables devices. Some do not have easily accessible data streams, including: Samsung Galaxy Watch, Xiaomi Mi Band, AmazFit, Suunto, and Coros. Some can have data partially accessed through the Apple HealthKit or Strava, but in that case we already have them 240 covered.

EEG headbands: We covered the Dreem Headband 3 in detail, but as the company was acquired and discontinued their helmet we have excluded it from our analysis. Other popular high-quality headbands include Hypnodyne Zmax 245 and OpenBCI, these are quite interesting but also very expensive.

Raw data access: Almost no commercially available device provides raw data access, Fitbit SDK gives some limited accelerometer/gyroscope for apps. OpenBCI offers EEG and PPG sensors with full access to sensors, which we have 250 note covered yet. Other research oriented wearable devices might do the same

Research wearable devices: We have tried to collaborate with wearable devices specifically designed for researchers, but it is cumbersome to access a single device for our purpose. Hopefully materializing this public platform allows research device companies to see the value and provide their device and API connectors to our open-source platform.

Use in clinical research

To run a distributed clinical study with wearables HIPAA compliance and a data risk assessment is required. The Wearipedia python package simplifies communication with wearable vendor. However, it is not a end-to-end solution. Wearable vendors have to be approved through individual data risk assessment. The Wearipedia python package has 255 to be stalled on a secure server and pipe the data into a secure and HIPAA approved database.

Human assays

- 260 For now, we have chosen to not pursue any human assays, even though in particular semen analysis is very easy to procure and well tested by now.

Ethics in research

We have seen that wearable devices offer unprecedented opportunities to capture real-time, high-quality data in decentralized clinical trials (DCTs) at little cost and limited patient burden. However, the use of wearables in DCTs also poses critical challenges that must be addressed to protect the rights and well-being of participants. a) Including minorities is pivotal in the early phases, in particular as the algorithms and methodologies developed in these early stages need to be as inclusive as possible, i.e. is a US\$800 Garmin watch necessary, or would a US\$100 Fitbit do just as well? Moreover, parameters such as melanin impacts PPG readings, and digital-readiness is not a given^{44,45}. b) Privacy concerns escalate when continuous data streams from wearable devices are transmitted via multiple platforms, in particular as most wearable vendors do not prohibit sharing data with unknown third-parties and dipping into on-device databases can be coerced without the participant realizing it. With easily derived features such as cycle, pregnancy status, heart issues, infectious disease status, and diabetes, it puts the participant at risk for partner violence, imprisonment under anti-abortion rulings, and being passed up for career opportunities or insurance company bias.^{45,46}. c) As most health issues are faced by an aging population the customer user base is mainly composed of the younger population that has adopted wearable technology. This could lead to an exclusion of the population most in need for novel wearable solutions⁴⁷. Conclusively, there's a need for a development of standards to ensure minorities and elderly are well represented in DCTs, with the low cost and ease of deployment this should be easier than ever. The more challenging task is to ensure privacy for individuals, in particular women of reproductive age, but as the algorithms keep getting better, possibly everyone. Current solutions are unfortunately quite limited as this would remove most commercially available products.

Data Sharing

Wearipedia python package: <https://github.com/Stanford-Health/Wearipedia>

Wearipedia website: <https://wearipedia.com>

CliniDigest: <https://github.com/Stanford-Health/CliniDigest>

- 285 Wearipedia data: <https://github.com/Stanford-Health/wearipedia-data>

Declaration of interests

Contributors

Alexander Johansen: Project lead, review of educational notebooks, website content

Kyu Hur: Website development, privacy and security section

- 290 **Jack Hung:** Wearipedia python package, notebooks: Polar H10/EliteHRV, Verity Sense, Abbott Freestyle Libre, NutriSense, Actigraph CentrePoint Insight

Rodrigo Castellon: Wearipedia python package, Whoop Strap, Withings ScanWatch, Body+, Sleep, Dreem Headband 3, Garmin Fenix, Dexcom CGM

Tristan Peng: Website development, CliniDigest

- 295 **Stephanie Ren:** Wearipedia python package, data extractors

Renee White: CliniDigest

Chanyeong Park: Platform for Clinical Researchers

Allison Lau: Fitbit, Garmin, Whoop Strap, Dexcom Pro CGM

Saarth Shah: Polar Vantage, Strava, Cronometer, MyFitnessPal

- 300 **Hee Jung Choi:** Biostrap, Qualtrics

William Wang: Whoop Strap, Withings ScanWatch, Body+, Sleep, Dreem Headband 3, Garmin Fenix, Dexcom CGM

Pann Sripitak: CliniDigest

Mohamed Elhusinni: Oura ring, Coros Pace

- 305 **Michael Snyder:** PI

Conflicts of interests

310 MPS is a cofounder and scientific advisor of Crosshair Therapeutics, Exposomics, Filtricine, Fodsel, iollo, InVu Health, January AI, Marble Therapeutics, Mirvie, Next Thought AI, Orange Street Ventures, Personalis, Protos Biologics, Qbio, RTHM, SensOmics. MPS is a scientific advisor of Abbratech, Applied Cognition, Enovone, Jupiter Therapeutics, M3 Helium, Mitrix, Neuvivo, Onza, Sigil Biosciences, TranscribeGlass, WndrHLTH, Yuvan Research. MPS is a cofounder of NiMo Therapeutics. MPS is an investor and scientific advisor of R42 and Swaza. MPS is an investor in Repair Biotechnologies. All other authors declare no competing interests.

Acknowledgments

315 This work was made possible by the support of the BV and Anu Jagadeesh Family Foundation. The authors would like to thank Helge Ræder for comments and review.

References

- 1 Li X, Dunn J, Salins D, Zhou G, Zhou W, Schüssler-Fiorenza Rose SM, et al. Digital health: tracking physiomes and activity using wearable biosensors reveals useful health-related information. *PLoS biology*. 320 2017;15(1):e2001402.
- 2 Quer G, Coughlin E, Villacian J, Delgado F, Harris K, Verrant J, et al. Feasibility of wearable sensor signals and self-reported symptoms to prompt at-home testing for acute respiratory viruses in the USA (DETECT-AHEAD): a decentralised, randomised controlled trial. *The Lancet Digital Health*. 2024;6(8):e546-54.
- 3 Marra C, Chen JL, Coravos A, Stern AD. Quantifying the use of connected digital products in clinical research. 325 *NPJ digital medicine*. 2020;3(1):50.
- 4 Shandhi MMH, Singh K, Janson N, Ashar P, Singh G, Lu B, et al. Assessment of ownership of smart devices and the acceptability of digital health data sharing. *NPJ digital medicine*. 2024;7(1):44.
- 5 Izmailova ES, Wagner JA, Perakslis ED. Wearable devices in clinical trials: hype and hypothesis. *Clinical Pharmacology & Therapeutics*. 2018;104(1):42-52.
- 6 Mishra T, Wang M, Metwally AA, Bogu GK, Brooks AW, Bahmani A, et al. Pre-symptomatic detection of COVID-19 from smartwatch data. *Nature biomedical engineering*. 2020;4(12):1208-20.
- 7 Radin JM, Quer G, Pandit JA, Gadaleta M, Baca-Motes K, Ramos E, et al. Sensor-based surveillance for digitising real-time COVID-19 tracking in the USA (DETECT): a multivariable, population-based, modelling study. *The Lancet Digital Health*. 2022;4(11):e777-86.
- 8 Maijala A, Kinnunen H, Koskimäki H, Jämsä T, Kangas M. Nocturnal finger skin temperature in menstrual cycle tracking: ambulatory pilot study using a wearable Oura ring. *BMC Women's Health*. 2019;19:1-10.
- 9 Grant A, Smarr B. Feasibility of continuous distal body temperature for passive, early pregnancy detection. *PLOS Digital Health*. 2022;1(5):e0000034.
- 10 Keeler Bruce L, González D, Dasgupta S, Smarr BL. Biometrics of complete human pregnancy recorded by 330 wearable devices. *NPJ Digital Medicine*. 2024;7(1):207.
- 11 Brandes A, Stavrakis S, Freedman B, Antoniou S, Boriani G, Camm AJ, et al. Consumer-led screening for atrial fibrillation: frontier review of the AF-SCREEN international collaboration. *Circulation*. 2022;146(19):1461-74.
- 12 Henriksen A, Woldaregay AZ, Muzny M, Hartvigsen G, Hopstock LA, Grimsgaard S. Dataset of fitness trackers and smartwatches to measuring physical activity in research. *BMC Research Notes*. 2022;15(1):258.
- 13 White R, Peng T, Sripitak P, Rosenberg Johansen A, Snyder M. Clinidigest: a case study in large language model based large-scale summarization of clinical trial descriptions. In: Proceedings of the 2023 ACM Conference on Information Technology for Social Good; 2023. p. 396-402.
- 14 Martin KD, Murphy PE. The role of data privacy in marketing. *Journal of the Academy of Marketing Science*. 2017;45:135-55.

- 350 15 Westin AF. Privacy and freedom. Washington and Lee Law Review. 1968;25(1):166.
- 16 Altman I. The environment and social behavior: privacy, personal space, territory, and crowding. 1975.
- 17 Rosenberg RS. The social impact of computers. Elsevier; 2013.
- 18 Nissenbaum H. Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press; 2020.
- 355 19 Warren SD, Louis D. Brandeis, The Right to Privacy, 4 Harv. L rev. 1890;193(10.2307):1321160.
- 20 Gavison R. Privacy and the Limits of Law. The Yale law journal. 1980;89(3):421-71.
- 21 Di Pietro R, Mancini LV. Security and privacy issues of handheld and wearable wireless devices. Communications of the ACM. 2003;46(9):74-9.
- 360 22 Thierer AD. The internet of things and wearable technology: Addressing privacy and security concerns without derailing innovation. Adam Thierer, The internet of things and wearable technology: Addressing privacy and security concerns without derailing innovation. 2015;21.
- 23 Ching KW, Singh MM. Wearable technology devices security and privacy vulnerability analysis. International Journal of Network Security & Its Applications. 2016;8(3):19-30.
- 24 Perez AJ, Zeadally S. Privacy issues and solutions for consumer wearables. It Professional. 2017;20(4):46-56.
- 365 25 McLennan M. The Global Risks Report 2021 16th Edition. World Economic Forum Cologny, Switzerland; 2021.
.
- 26 Al-Muhtadi J, Mickunas D, Campbell R. Wearable security services. In: Proceedings 21st International Conference on Distributed Computing Systems Workshops. IEEE; 2001. p. 266-71.
- 370 27 Seneviratne S, Hu Y, Nguyen T, Lan G, Khalifa S, Thilakarathna K, et al. A survey of wearable devices and challenges. IEEE Communications Surveys & Tutorials. 2017;19(4):2573-620.
- 28 Callaghan M, Harkin J, McGinnity T, et al. Case study on the Bluetooth vulnerabilities in mobile devices. IJCSNS International Journal of Computer Science and Network Security. 2006;6(4):125-9.
- 29 Hale ML, Lotfy K, Gamble RF, Walter C, Lin J. Developing a platform to evaluate and assess the security of wearable devices. Digital Communications and Networks. 2019;5(3):147-59.
- 375 30 Commission FT, Commission FT, et al.. Developer of popular women's fertility-tracking app settles FTC allegations that it misled consumers about the disclosure of their health data. Press Release. Available at: <https://www.ftc.gov/news-events/press>; 2021.
- 31 Kirk S. The Wearables Revolution: Is Standardization a Help or a Hindrance?: Mainstream technology or just a passing phase? IEEE Consumer electronics magazine. 2014;3(4):45-50.
- 380 32 Ravi D, Wong C, Lo B, Yang GZ. A deep learning approach to on-node sensor data analytics for mobile or wearable devices. IEEE journal of biomedical and health informatics. 2016;21(1):56-64.
- 33 Greiwe J, Nyenhuis SM. Wearable technology and how this can be implemented into clinical practice. Current allergy and asthma reports. 2020;20:1-10.
- 34 Chandrasekaran R, Katthula V, Moustakas E. Patterns of use and key predictors for the use of wearable health care devices by US adults: insights from a national survey. Journal of medical Internet research. 2020;22(10):e22443.
- 385 35 Mehraeen E, Ghazisaeedi M, Farzi J, Mirshekari S. Security challenges in healthcare cloud computing: a systematic review. Global journal of health science. 2016;9(3):157.
- 36 Bansal G, Gefen D, et al. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. Decision support systems. 2010;49(2):138-50.

- 390 37 Banerjee S, Hemphill T, Longstreet P. Wearable devices and healthcare: Data sharing and privacy. The Information Society. 2018;34(1):49-57.
- 38 Act A. Health insurance portability and accountability act of 1996. Public law. 1996;104:191.
- 39 Theodos K, Sittig S. Health information privacy laws in the digital age: HIPAA doesn't apply. Perspectives in health information management. 2021;18(Winter).
- 395 40 Koçi R, Franch X, Jovanovic P, Abelló A. A data-driven approach to measure the usability of web APIs. In: 2020 46th Euromicro Conference on Software Engineering and Advanced Applications (SEAA). IEEE; 2020. p. 64-71.
- 41 Lomborg S, Bechmann A. Using APIs for data collection on social media. The Information Society. 2014;30(4):256-65.
- 42 Badhwar R. Intro to API Security-Issues and Some Solutions! In: The CISO's Next Frontier: AI, Post-Quantum Cryptography and Advanced Security Paradigms. Springer International Publishing Cham; 2021. p. 239-44.
- 400 43 Muratyan A, Cheung W, Dibbo SV, Vhaduri S. Opportunistic multi-modal user authentication for health-tracking IoT wearables. In: The Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021. Springer; 2022. p. 1-18.
- 44 Zinzuwadia A, Singh JP. Wearable devicesâaddressing bias and inequity. The Lancet Digital Health. 2022;4(12):e856-7.
- 405 45 Figueroa CA, Luo T, Aguilera A, Lyles CR. The need for feminist intersectionality in digital health. The Lancet Digital Health. 2021;3(8):e526-33.
- 46 Vayena E, Blasimme A, Sugarman J. Decentralised clinical trials: ethical opportunities and challenges. The Lancet Digital Health. 2023;5(6):e390-4.
- 410 47 Guu TW, Muurling M, Khan Z, Kalafatis C, Aarsland D, Brem AK, et al. Wearable devices: underrepresentation in the ageing society. The Lancet Digital Health. 2023;5(6):e336-7.

Appendix A. Website and Database — Submission Walk-through

Overview

To submit a device to the Wearipedia is a multistep process, first a device connector needs to be accepted, then an educational notebook, then CliniDigest and finally clinical and security evaluations. Device connector - The Wearipedia python package The wearipedia python package is hosted in an open-source Github project at <https://github.com/stanford-health/wearipedia> and details on submitting pull-requests to the repository are presented here. A functional data connector conveniently wraps the Application Programming Interface (API) or Software Development Kit (SDK) of the vendor to access data resulting in an easy-to-use interface.

415 420 A connector must have a simulator for key data types. This is to reduce unnecessary sharing of user credentials when building educational content and testing devices.

Educational notebook

The Wearipedia project has a set of educational open-source notebooks at <https://github.com/Stanford-Health/wearable-notebooks>. The notebooks are written in python and details how to extract and conduct clinical research using the wearable. To submit a notebook it should follow the general style of: https://github.com/Stanford-Health/wearable-notebooks/blob/main/notebooks/fitbit_charge_6.ipynb which includes: A 1-page letter detailing setup for the user, and a formal guide of what is expected of the user in the remainder of the clinical study. A setup guide for the clinical researcher to ensure access to data for one user. Data extraction using the Wearipedia python package for one user. Data simulation using the Wearipedia python package Guide on how to port data to R, Matlab, Excel, and standard data formats using the Wearipedia python package. Minimum 2 plots visualizing details of data Guide, and visualization, on how to remove non-adherence for a custom period and custom adherence percentage (e.g. days, weeks, months). Guide, and visualization, on how to remove outliers using statistical testing. Guide, and visualization, on how to test a hypothesis.

CliniDigest

- 435 CliniDigest provides overviews of wearable usage in current clinical studies sorted by medical fields. A natural language processing tool that extracts clinical trials from <https://clinicaltrials.gov>, then filters based on search terms (e.g. Fitbit), classifies across 14 clinical topics, and writes a summary using LLMs such as ChatGPT. To include a wearable the only requirement is to upload the additional search terms. Guidelines can be found at <https://github.com/Stanford-Health/CliniDigest>.

440 Privacy and Security

- The Wearipedia provides a privacy and security evaluation of 25 wearable devices in the main text under Table 3. Guidelines can be found at <https://github.com/Stanford-Health/wearipedia-data>. The metrics are fully outlined under Appendix D and the source material for these evaluations can include the privacy policy, terms of service, or other gray literature provided by the company. To submit the privacy and security evaluations of a new device, a pull request can be opened according to the instructions outlined in the repository's README.

Appendix B. Wearipedia Python Package

Wearipedia is a Python package designed to standardize and simplify the process of interfacing with wearable devices. The package is built with modern software engineering practices and follows a modular, extensible architecture.

Package Architecture

- 450 Wearipedia defines a device-agnostic abstraction layer that allows for easy integration of a new wearable device. The base of the package is the definition of the device interface, which defines the required methods that must be implemented by each new device. Each implementation follows the standardized interface while making device-specific optimizations.

One of the core pieces of each implementation is authentication. Because different devices use different protocols 455 such as OAuth 2.0, OAuth 1.0, or basic authentication with username and password, each authentication per device type must be implemented separately with the right endpoints and parameters. For some devices, there is both an interactive and non-interactive version of authentication. The interactive version can be used in a user-friendly manner to prompt users through the authentication process, which may include clicking a link to the application and granting access. The non-interactive version can still be used to authenticate programmatically as needed.

- 460 On initialization, each device implementation must specify its valid data types for types of data that can be requested. It must also implement data access through a `get_data` method. Each implementation should take in a standardized format of inputs such as YYYY-MM-DD dates as well as return outputs using standardized units. Devices are implemented to have both a real and synthetic data setting. The real setting queries for real user data and the synthetic setting generates fake data that can be used to develop data analysis code without accessing user data. Each device implementation should include tests for both the real and synthetic settings.

The package also includes a command line interface (CLI) mode which provides a user-friendly interface for interacting with data through Wearipedia.

Appendix B.1. Technical Implementation Details

Appendix B.1.1. Development Environment

- 470 The package is supported for Python 3.9+ (except Garmin access, which is only supported in 3.10+) and follows modern development practices:

1. Dependency Management: Utilizes Poetry for dependency management and version control
2. Code Quality: Implements pre-commit hooks for code formatting and static analysis
3. Testing Framework: Comprehensive test suite using pytest, with coverage tracking
4. Documentation: Sphinx-based documentation system with ReadTheDocs integration

475 We chose to use Python for the development language due to its popularity for data analysis in research applications.

Appendix B.2. Design Decisions

Modularity: The package is designed with clear separation of concerns, allowing for:

1. Independent development of device drivers
2. Easy maintenance and updates

480

User Experience

1. Intuitive API design with consistent method naming
2. Clear parameter documentation
3. Type hints for better IDE integration
4. Comprehensive error messages
5. CLI interface
6. Wrappers around provided API functionality; e.g. combining multiple pages of data from paginated queries

485

Appendix C. Clinical Trial Tracking

CliniDigest aims to provide clinical trial coordinators with easy and concise access to recent clinical trial developments. As such, it is imperative to use specific criteria for which clinical trials to include. Considering the date of the last update posted, enrollment count, and study status, the pipeline utilizes two complementary criteria for including a clinical trial. The criteria for a clinical trial to be included is as follows:

490

Option 1: New trials

- Last Update Posted: 2 years ago — today
- Enrollment Count: ≥ 25
- Study Status (one of): Recruiting, Enrolling by Invitation, Active Not Recruiting, Not Yet Recruiting, Suspended, Completed

495

Option 2: Current trials

500

- Last Update Posted: 5 years ago — 2 years ago
- Enrollment Count: ≥ 25
- Study Status (one of): Recruiting, Enrolling by Invitation, Active Not Recruiting

505

From the clinical trials that fit within the criteria to be searched, the regular expressions defined in the pipeline are checked for matches within each clinical trial's data. For each medical device, it is necessary to identify the best search terms to identify clinical trials that use the given medical device. In order to do so, follow the steps detailed at <https://github.com/Stanford-Health/CliniDigest>. After identifying all clinical trials that use a wearable device, they are classified into fourteen medical fields. Each combination of a wearable device and medical combination with at least one clinical trial is then summarized using engineered prompts and OpenAI's gpt-4-0125-preview model. The default summary length requested is 150-250 words. The summary length is shortened to 50-150 words if there are five or fewer clinical trials. Below are three examples: one with fewer than five trials, one with an average number of trials, and one with over two hundred trials.

510

The purpose of a Polar H in pulmonology trials is to provide a reliable and non-invasive method for monitoring and assessing cardiovascular responses to various rehabilitation interventions in patients with respiratory conditions. By measuring heart rate variability and other hemodynamic responses, the Polar H facilitates the evaluation of the immediate effects of innovative exercise modalities, such as high-intensity interval exercises in children with asthma [1], and supports the safety and efficacy assessment of novel rehabilitation interventions like low-intensity exercise with blood flow restriction in COPD patients [2]. This technology is crucial for tailoring and optimizing pulmonary rehabilitation programs to enhance patient outcomes.

515

Example 1: Example of CliniDigest for the Polar H on Pulmonology. Out of 3 studies, 2 are selected and used for the summary.

520

The Garmin Fenix, a sophisticated wearable technology, is increasingly being integrated into oncology trials to enhance patient monitoring, improve quality of life (QoL), and facilitate personalized interventions. Its purpose in these trials is multifaceted, primarily focusing on the collection of real-world data (RWD) to monitor physical activity, sleep quality, and heart rate, which are critical parameters in assessing the overall health and well-being of cancer patients [2][3]. For instance, in the REBECCA-2 study, the Garmin Fenix is utilized to gather RWD, enabling personalized follow-up care aimed at improving the QoL of breast cancer survivors by detecting signs of QoL deterioration and facilitating timely interventions [2]. Similarly, the eCAN JA project employs this device to automatically collect physical parameters, supporting tele-rehabilitation and tele-psychological support programs that aim to empower patients and improve their QoL through enhanced remote monitoring [3]. Moreover, the device's role extends to pediatric oncology, where it aids in measuring recovery post-surgery through smartwatch data and questionnaires, highlighting its versatility across different age groups and cancer types [7]. The Garmin Fenix's ability to seamlessly integrate into patients' lives while providing valuable health metrics positions it as a pivotal tool in modern oncology trials, driving forward the paradigm of personalized and remote patient care.

Example 2: Example of CliniDigest for the Garmin Fenix on Oncology. Out of 20 studies, 3 are selected and used for the summary.

The Dexcom G Pro, a continuous glucose monitoring (CGM) system, plays a pivotal role in advancing endocrinology trials by providing accurate, real-time glucose level data across various patient populations and conditions. Its purpose extends beyond mere glucose tracking; it serves as a critical tool in evaluating the efficacy and safety of diabetes management strategies, understanding the glycemic impact of pharmaceutical interventions, and exploring the physiological nuances of diabetes and its comorbidities. For instance, in trials evaluating the safety and effectiveness of automated insulin delivery systems in children and adults with type 1 diabetes, the Dexcom G Pro's continuous glucose data is indispensable for assessing system performance in real-world settings [13][195]. Similarly, its use in studies exploring the impact of dietary interventions on glycemic control underscores its utility in non-pharmacological diabetes research [179]. Moreover, the Dexcom G Pro facilitates the investigation of glycemic variability and its clinical implications in conditions like polycystic ovary syndrome, thereby broadening our understanding of glucose dynamics beyond diabetes [170]. In the context of hospital care, its application in monitoring hospitalized patients with diabetes highlights its potential to improve inpatient glycemic management and reduce the risk of hypoglycemia [192]. Collectively, the Dexcom G Pro's integration into endocrinology trials underscores its critical role in enhancing diabetes care through rigorous research, ultimately contributing to the development of personalized, data-driven treatment approaches that can significantly improve patient outcomes.

Example 3: Example of CliniDigest for the Dexcom G Pro on Endocrinology. Out of 206 studies, 5 are selected and used for the summary.

Appendix D. Privacy and Security

Full descriptions of every metric under privacy and security provided in Table 1 are listed below. For each rating, a metric description elucidates the context and need for each rating, then a recommended performance which determines the threshold of whether the wearable passes or fails that category is described. 25 different wearables are graded on these 7 ratings in Table 3.

Appendix D.1. Metric Description — Low Data Risk

Wearable devices collect highly sensitive personal data—sleep quality, activity levels, heart rate, glucose readings and location—which, if mismanaged, can cause serious harm to users¹⁻⁴. Such primary data are straightforward to measure but demand strict controls. Beyond what is directly recorded, predictive data health risk scores, fitness estimates, lifestyle or behavioral patterns, mood or disease onset predictions can be inferred from primary signals. As inference methods advance, even innocuous measurements may reveal deeply personal insights⁵⁻⁸. This growing inferential power makes true anonymization impossible^{9,10}. Some examples include body temperature for tracking period cycles or pregnancy⁸, heart rate for early COVID-19 detection¹¹, and location for stalking or harassment¹²⁻¹⁴. Primary data

570 categories commonly collected include physical activity (steps, distance, calories, pace, MET-minutes)^{15,16}, physiologically (heart rate variability, blood pressure, SpO₂, skin temperature)¹⁷, sleep metrics (total sleep time, stages, interruptions, efficiency)¹⁸, and health status (glucose, hydration, BMI, menstrual tracking)^{19,20}. Predictive data examples include health risk assessments (e.g. diabetes, cardiovascular disease)^{21,22}, fitness metrics (VO₂ max, recovery time)^{23,24}, lifestyle and behavioral patterns (sleep habits, social interaction, sedentary time)^{25,26}, and health insights (flu onset, mood, fatigue)²⁷. Under privacy frameworks (HIPAA, GDPR), the highest risk categories are primary
575 physiological, sleep and health status data, plus predictive health assessments and insights^{28,29}. Misuse by insurers, employers or malicious actors can lead to discrimination, social stigma, psychological distress and financial loss^{30,31}.

Recommended Performance

Wearable vendors should limit collection to only what is strictly necessary and implement robust safeguards across both primary and predictive data.

580 **Appendix D.2. Metric Description — Compliant with HIPAA**

The Health Insurance Portability and Accountability Act (HIPAA), enacted in 1996, established comprehensive standards for protecting patient health information and was strengthened by the 2009 HITECH amendment to cover electronic health records, earning praise for its detailed privacy safeguards in practice^{28,32,33}. As consumer wearables generate increasingly diverse and granular data streams, experts have called for HIPAA's scope to expand to include
585 sensor-derived information and for its provisions to be updated accordingly^{34,35}. Under current rules, de-identification mandates suppression of 18 direct and indirect identifiers before any dataset release, and patient consent is required for disclosures of identifiable information²⁸. Large scale anonymized repositories—such as NHANES—demonstrate how stripping these identifiers can enable valuable research while ostensibly preserving privacy³⁶. However, numerous high-profile cases have shown that anonymized health data can be re-identified by linking with external sources:
590 the Netflix Prize dataset was deanonymized through auxiliary movie ratings³⁷, AOL search logs revealed user identities³⁸, and medical records spurred the development of k-anonymity models after re-identification of supposedly private health data^{39,40}. Wearable-derived datasets demonstrate volume, frequency, as well as richness and can face even greater re-identification risks^{41,42}. To mitigate these vulnerabilities, wearable manufacturers should limit collection of HIPAA identifiers, apply robust de-identification techniques in line with HIPAA's Privacy Rule, restrict data sharing to essential uses with explicit user consent, and acknowledge that no anonymization can be entirely foolproof.
595

Recommended Performance

Vendors should not collect any HIPAA identifiers.

Any data that falls under what is outlined as a HIPAA identifier would make a device non-HIPAA compliant. While most wearable devices are not covered under HIPAA, this law provides a comprehensive legal framework to determine
600 what may be important identifying data that wearable devices should collect with explicit consent. The following categories of data are defined as HIPAA identifiers (comma delimited): Name, Address, All elements of dates related to an individual, Telephone numbers, Fax number, Email address, Social security number, Medical record number, Health plan beneficiary number, Account number, Certificate or license number, Vehicle identifiers and serial numbers, Device identifiers and serial numbers, Web URL, Internet protocol address, Finger or voice print, Photographic image, and Any other characteristic that could uniquely identify the individual.
605

Appendix D.3. Metric Description — De-identifies Data When Sharing

Public datasets offer significant benefits by increasing the amount of available data, yet this often comes at the cost of individual privacy. Organizations frequently de-identify data—that is, remove sensitive personal information while retaining other useful details—to mitigate privacy risks⁴³. De-identification performed at the time of data collection
610 reduces the likelihood of exposing sensitive information, thereby enhancing user privacy protection. However, re-identification of anonymized data is emerging as a serious concern. A 2016 report documented a 320% increase in hacking attacks on healthcare providers, and the volume and detail of wearable data only exacerbate these vulnerabilities⁴⁴. Conventional de-identification techniques such as k-anonymity^{45,46}, l-diversity^{39,47}, and t-closeness^{39,45} each present unique challenges in preventing re-identification, highlighting the need for continued innovation in privacy protection methods.
615

Recommended Performance

The vendor should de-identify the data before sharing with other entities.

By nature of the request, it would be impossible to determine what de-identification method is utilized by vendors. Any data that can be tied to health data should be de-identified before sharing.

620 Appendix D.4. Metric Description — No Third Party Sharing

Most wearable manufacturers include clauses about sharing data with third-party vendors, who in turn may use the data for purposes outside the explicit consent provided by users. Numerous service policies evaluated in this review include general third-party data-sharing provisions from major vendors such as Apple and Google's Fitbit^{48–50}. In addition, few vendors explain which third-party services gain access to users' personal data or why such access is granted; instead, 625 they rely on broad, all-encompassing language to account for potential future actions⁵¹. Furthermore, many policies include provisions that allow sharing identifiable information when required by law, which could lead to harmful legal repercussions for users. Tech policy researchers in the United States have warned of the potential privacy invasions by period-tracking apps following the overturning of Roe v. Wade^{52–55}. Overall, sharing data with third parties can pose significant risks to a user's privacy.

630 Recommended Performance

The vendor should not share data with third parties.

Appendix D.5. Metric Description — Transparency in Third Party Sharing

Vendors must fully inform users about all data sharing practices and the underlying intent. Ard (2013)⁵⁶ argues that it is increasingly difficult to identify and regulate third parties because they are not obligated to adhere to the privacy 635 agreements established between users and vendors. The study proposes that certain types of information should remain confidential regardless of who may acquire it. However, this approach necessitates that both users and regulators are aware of all third parties that receive user data, thereby requiring complete transparency and disclosure. Notably, a vendor that does not share data with any third party would automatically be considered fully compliant with these privacy standards.

640 Recommended Performance

The vendor should disclose all third parties that receive user data. Any language of data sharing with vague or unspecified third parties is considered not transparent.

In one study, human annotators determined the top 5 vague words in privacy policies to be "may", "personal information", "information", "other", and "some"⁵⁷. Another study analyzed mobile health and fitness apps to find that 645 privacy policies were frequently not applied to third-party links and services⁵⁸. One researcher goes as far as to coin the term "Incognito Problem" to refer to users being provided little to no information on which third parties obtain user data⁵⁹.

If a vendor does not share data with third parties, the vendor is awarded this metric automatically.

Appendix D.6. Metric Description — Secure Wearable Connectivity

650 Wearable devices rely almost entirely on wireless communication—a technology that began gaining traction before the turn of the millennium⁶⁰ and has since become the primary method for device-to-device connectivity^{61,62}. A variety of wireless protocols, such as WiFi, ZigBee, Z-Wave, Sigfox, Neul, LoRaWAN, RFID, NFC, GSM/3G/4G, Bluetooth LE, GLoWPAN, HomePlug, Thread, DSRC, and WiMax, are used by IoT devices, each presenting different levels of security vulnerabilities^{63,64}. Among these, Bluetooth LE is the most popular and practical communication protocol 655 for the majority of wearable devices on the market^{65,66}. However, vulnerabilities in these wireless connections or in pre-authorized smartphone applications can be exploited by malicious actors to access sensitive data^{67–70}.

Between Bluetooth LE and WiFi, Bluetooth LE is favored for its lower energy consumption and suitability for resource-limited devices, but it is vulnerable to man-in-the-middle attacks which can lead to significant security risks⁶⁸. Common Bluetooth attacks include bluesnarfing, eavesdropping, and packet injection^{68,69}. Since wearables often serve as entry points for hackers, compromising these devices can also expose smartphones or computers to broader security breaches⁷¹.

On the other hand, WiFi is generally considered more secure than Bluetooth despite both employing 128-bit encryption, because WiFi tends to employ certificate-based, server-backed authentication frameworks (WPA2 or WPA3

Enterprise)^{67,72}. Although WiFi is not free from vulnerabilities—as seen in the 2016 botnet attacks that compromised millions of devices⁷³—transmitting wearable data via WiFi is highly recommended. That said, the security of WiFi is highly dependent on the user's network configuration. Users should ensure they connect through WPA-2 or WPA-3 networks since WEP is known to have significant security weaknesses^{74,75}. Users are also susceptible to remote attacks that would typically not be a risk for local connection protocols.

Recommended Performance

670 Wearable devices should be capable of connecting through WiFi.

Wearable devices use several methods to communicate, including ANT/ANT+, Near Field Communication (NFC), Bluetooth/Bluetooth Low Energy (BLE), Zigbee/Thread/Z-Wave, WiFi, and Cellular (3G/4G/5G). However, the security of networking protocols in wearable devices depends highly on both implementation and specific use case. Protocol-level defaults (i.e. design specifications) determine the base level for certain standards⁷⁶, vendor implementation influence whether devices have encryption or robustly secure keys (e.g. assigning unique identifiers for advertising purposes—increasing risk of long-term tracking⁷⁷), and client-sided factors such as a user connecting over an unencrypted network. Ranking network protocols is largely difficult due to the concerted nature of establishing a secure network (protocol, vendor, user/client) and a single point of failure in adherence of the three could expose vulnerabilities. However, the proposed ranking (from least to most secure) based on protocol characteristics, default settings, and other one-off considerations are as follows:

- **ANT/ANT+:** Not encrypted by default, no built-in authentication, AES-128 is optional and by way of single-channel communications^{78,79}.
- **NFC:** Offers fast, secure pairing with man-in-the-middle resistance, but can be vulnerable to eavesdropping, data modification, and tracking⁸⁰ especially if an attacker can get physically close—but also requires an attacker to get close⁸¹. No confidentiality guarantees by default⁸²
- **Bluetooth/BLE:** Although these protocols incorporate security measures, implementation is left to device manufacturers and there are known security issues⁸³.
- **Zigbee/Thread/Z-Wave:** Security is dependent on the implementation by the manufacturer⁸⁴.
- **WiFi:** Offers strong security, especially with WPA2 and WPA3, but because it is implemented locally it increases the potential for remote attacks⁸⁵.
- **Cellular (3G/4G/5G):** Managed by telecom companies that adhere to stringent security regulations, offering robust protection⁸⁶.

Appendix D.7. Metric Description — Secure API Access

Permissions to access data storages are typically provided through APIs or SDKs developed by device manufacturers. 695 APIs serve as tools for applications to interact with each other, while SDKs package these API methods for similar functionality. These interfaces can be either public, allowing any internet-connected entity to access data, or private, restricting access to select entities within a controlled network. Many modern applications, including wearable platforms, depend on APIs for authentication and data access⁸⁷. When a vendor offers a public API, users can download data stored on company servers from anywhere in the world⁸⁸. However, before any data is accessed, authentication and authorization protocols are required to ensure that only authorized users gain entry⁶³. Among the various protocols available, OAuth 2.0 has become the de facto gold standard for authorization due to its robust authentication and authorization properties, despite having its own security vulnerabilities⁸⁹.

Recommended Performance

705 Vendors should utilize the OAuth 2.0 protocol (or more secure protocol, explained below) when exposing data through APIs.

Below is a list of common authentication and authorization protocols used for API data access ranked from least to most secure. This is followed by an explanation of which performance attributes are desirable.

- **Basic Authentication:** Sends Base64-encoded credentials with every request; vulnerable to man-in-the-middle attacks unless used over HTTPS⁹⁰.
- **Digest Authentication:** Transmits a hashed password instead of plain text but still vulnerable to man-in-the-middle attacks and lacks password salting⁹¹.

- 715
- **API Key Authentication:** Assigns a unique key per user that is included in each API call; simple but risky if the key is exposed^{92,93}.
 - **OAuth 1.0:** Utilizes cryptographic signatures with a shared secret for authorization; more secure than earlier methods yet complex and largely superseded⁹⁴.
 - **OAuth 2.0:** The industry standard for authorization, offering tailored flows for various platforms and balancing strong security with developer simplicity^{95–97}.
 - **OpenID Connect (OIDC):** Adds an identity verification layer on top of OAuth 2.0, enabling clients to confirm the end-user's identity and access profile information⁹⁷.
 - **Mutual TLS (mTLS):** Extends TLS by requiring both client and server authentication, providing the highest level of security despite higher computational overhead⁹⁸.
- 720

Effective API access protocols must balance robust security with efficiency. OAuth 2.0 is widely adopted because they offer strong security without significantly impacting performance, making them suitable for modern, distributed applications. Thus, we recommend that vendors utilize the OAuth 2.0 protocol (or more secure protocols mentioned above such as OIDC or mTLS) when exposing data through APIs.

725

Privacy and Security Rating Citations

Sources for how each privacy and security rating was graded is provided in Table D.4. Most of the sources used to rate wearables were privacy policies, terms of use agreements, or manuals provided by each vendor. This is largely satisfactory due to the legally binding nature of these use agreements between users and vendors. While incidents have occurred of vendors violating these agreement policies, few if any third parties can accurately verify whether a vendor is violating their own terms of use agreements and is therefore a limitation of these ratings.

Company	Model Name	Low Data Risk	Compliant with HIPAA	De-identifies Data When Sharing	No Third Party Sharing	Transparency in Third Party Sharing	Secure Wearable Connectivity	Secure API Access
Abbott	Freestyle Libre 2	99	99–101	99	99	99	102	100
Actigraph	CentrePoint Insight	103–105	103	103	103	103	106	107
Apple	Health kit	108	109	109,110	109	109	—	111
Apple	Watch 5	108	109	109,110	109	109	112	111
Apple	Watch Ultra	113–116	109	109,110	109	109	117	118
Apple	iPhone	113,119–121	109,122–124	110,125–127	109	109	117	—
Coros	Pace 2	128	128	128	128	128	129	—
Dexcom	Pro CGM	130	131	131	131	131	132	130,133
Fitbit	Sense	134	134	134	134	134	135	136
Fitbit	Charge 4	134	134	134	134	134	135	136
Garmin	Fenix 7S	137–140	137	141–143	137	137	144	145
Nutrisense	CGM Patch	146	146	146	146	146	147	—
Oura	Ring 3	148	149	150	151	151	152,153	154
Polar	H10	155	155	155	155	155	156	157
Polar	Vantage 2	155,158	155	155	155	155	159	157
Polar	Verity Sense	155,160	155	155	155	155	160,161	157
SleepOn	go2sleep	162	162	162	162	162	163	—
Suunto	HR Monitor	164	165	165	165	165	166	167
Whoop	Strap 4.0	168	138,140,169,170	169	169	169	169	171,172
Withings	Body+	173	173	173	173	173	174	175
Withings	ScanWatch	173,176	173	173	173	173	177	175,178
Withings	Sleep	173	173	173	173	173	179	175
-	Cronometer	180	180	180	180	180	—	—
-	MyFitnessPal	181	181	181	181	181	—	182
-	Strava	183	183	183	183	183	—	184

Table D.4: Citations for Table 3. Each source was accessed within the last year (2024 onwards) and scoured for language that provides evidence of meeting or failing the rating (as expressed under recommended performance in Appendix D). A dashed line indicates that result is not applicable or a source could not be provided.

References

- 735 1 Jain SH, Powers BW, Hawkins JB, Brownstein JS. The digital phenotype. *Nature biotechnology*. 2015;33(5):462-3.
- 2 Peake JM, Kerr G, Sullivan JP. A critical review of consumer wearables, mobile applications, and equipment for providing biofeedback, monitoring stress, and sleep in physically active populations. *Frontiers in physiology*. 2018;9:743.
- 740 3 Henriksen A, Haugen Mikalsen M, Woldaregay AZ, Muzny M, Hartvigsen G, Hopstock LA, et al. Using fitness trackers and smartwatches to measure physical activity in research: analysis of consumer wrist-worn wearables. *Journal of medical Internet research*. 2018;20(3):e110.
- 4 Kim J, Campbell AS, Wang J. Wearable non-invasive epidermal glucose sensors: A review. *Talanta*. 2018;177:163-70.
- 745 5 Shmueli G. To explain or to predict? 2010.
- 6 O'neil C. Weapons of math destruction: How big data increases inequality and threatens democracy. Crown; 2017.
- 7 Selbst AD, Barocas S. Big dataâs disparate impact. *California Law Review*. 2016;104(3).
- 8 Grant A, Smarr B. Feasibility of continuous distal body temperature for passive, early pregnancy detection. *PLOS Digital Health*. 2022;1(5):e0000034.
- 750 9 De Montjoye YA, Radaelli L, Singh VK, Pentland Aâ. Unique in the shopping mall: On the reidentifiability of credit card metadata. *Science*. 2015;347(6221):536-9.
- 10 Rocher L, Hendrickx JM, De Montjoye YA. Estimating the success of re-identifications in incomplete datasets using generative models. *Nature communications*. 2019;10(1):3069.
- 11 Alavi A, Bogu GK, Wang M, Rangan ES, Brooks AW, Wang Q, et al. Real-time alerting system for COVID-19 and other stress events using wearable data. *Nature medicine*. 2022;28(1):175-84.
- 755 12 Bowles N. Thermostats, locks and lights: Digital tools of domestic abuse. *The New York Times*. 2018;23.
- 13 Woodlock D. The abuse of technology in domestic violence and stalking. *Violence against women*. 2017;23(5):584-602.
- 14 Boorstein M, Iati M, Shin A. Top US Catholic Church official resigns after cellphone data used to track him on Grindr and to gay bars. *The Washington Post*. 2021.
- 760 15 Evenson KR, Goto MM, Furberg RD. Systematic review of the validity and reliability of consumer-wearable activity trackers. *International Journal of Behavioral Nutrition and Physical Activity*. 2015;12:1-22.
- 16 Doherty A, Jackson D, Hammerla N, Plötz T, Olivier P, Granat MH, et al. Large scale population assessment of physical activity using wrist worn accelerometers: the UK biobank study. *PloS one*. 2017;12(2):e0169649.
- 765 17 Kim J, Campbell AS, de Ávila BEF, Wang J. Wearable biosensors for healthcare monitoring. *Nature biotechnology*. 2019;37(4):389-406.
- 18 De Zambotti M, Cellini N, Goldstone A, Colrain IM, Baker FC. Wearable sleep technology in clinical and research settings. *Medicine and science in sports and exercise*. 2019;51(7):1538.
- 19 dos Santos CC, Lucena GN, Pinto GC, Júnior MJ, Marques RF. Advances and current challenges in non-invasive wearable sensors and wearable biosensorsâA mini-review. *Medical Devices & Sensors*. 2021;4(1):e10130.
- 770 20 Lyzwinski L, Elgendi M, Menon C. Innovative approaches to menstruation and fertility tracking using wearable reproductive health technology: systematic review. *Journal of medical Internet research*. 2024;26:e45139.

- 21 Perez MV, Mahaffey KW, Hedlin H, Rumsfeld JS, Garcia A, Ferris T, et al. Large-scale assessment of a smart-watch to identify atrial fibrillation. *New England Journal of Medicine*. 2019;381(20):1909-17.
- 775 22 Huang JD, Wang J, Ramsey E, Leavey G, Chico TJ, Condell J. Applying artificial intelligence to wearable sensor data to diagnose and predict cardiovascular disease: a review. *Sensors*. 2022;22(20):8002.
- 23 Altini M, Casale P, Penders J, Ten Velde G, Plasqui G, Amft O. Cardiorespiratory fitness estimation using wearable sensors: Laboratory and free-living analysis of context-specific submaximal heart rates. *Journal of applied physiology*. 2016;120(9):1082-96.
- 780 24 Shandhi MMH, Bartlett WH, Heller JA, Etemadi M, Young A, Plötz T, et al. Estimation of instantaneous oxygen uptake during exercise and daily activities using a wearable cardio-electromechanical and environmental sensor. *IEEE journal of biomedical and health informatics*. 2020;25(3):634-46.
- 25 Ringeval M, Wagner G, Denford J, Paré G, Kitsiou S. Fitbit-based interventions for healthy lifestyle outcomes: systematic review and meta-analysis. *Journal of medical Internet research*. 2020;22(10):e23954.
- 785 26 Uddin MZ, Soylu A. Human activity recognition using wearable sensors, discriminant analysis, and long short-term memory-based neural structured learning. *Scientific Reports*. 2021;11(1):16455.
- 27 Radin JM, Wineinger NE, Topol EJ, Steinhubl SR. Harnessing wearable device data to improve state-level real-time surveillance of influenza-like illness in the USA: a population-based study. *The Lancet Digital Health*. 2020;2(2):e85-93.
- 28 Act A. Health insurance portability and accountability act of 1996. *Public law*. 1996;104:191.
- 790 29 GDPR G. EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1. EC (General Data Protection Regulation) OJ L 119. 2016;1.
- 30 Mittelstadt BD, Floridi L. The ethics of biomedical big data. vol. 29. Springer; 2016.
- 795 31 Cohen IG, Amarasingham R, Shah A, Xie B, Lo B. The legal and ethical concerns that arise from using complex predictive analytics in health care. *Health affairs*. 2014;33(7):1139-47.
- 32 Solove DJ. HIPAA mighty and flawed. *Journal of AHIMA*. 2013;84(4):30-1.
- 33 Cohen IG, Mello MM. HIPAA and protecting health information in the 21st century. *Jama*. 2018;320(3):231-2.
- 800 34 Lecher C. The FDA Doesn't Want to Regulate Wearables, and Device Makers Want to Keep It That Way. *The Verge*. 2015.
- 35 Papandrea P. Addressing the HIPAA-potamus sized gap in wearable technology regulation. *Minn L Rev*. 2019;104:1095.
- 36 Fain JA. NHANES: use of a free public data set. SAGE Publications Sage CA: Los Angeles, CA; 2017.
- 805 37 Narayanan A, Shmatikov V. Robust de-anonymization of large sparse datasets. In: 2008 IEEE Symposium on Security and Privacy (sp 2008). IEEE; 2008. p. 111-25.
- 38 Barbaro M, Zeller T, Hansell S. A face is exposed for AOL searcher no. 4417749. *New York Times*. 2006;9(2008):8.
- 810 39 Samarati P, Sweeney L. Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression. 1998.
- 40 Na L, Yang C, Lo CC, Zhao F, Fukuoka Y, Aswani A. Feasibility of reidentifying individuals in large national physical activity data sets from which protected health information has been removed with use of machine learning. *JAMA network open*. 2018;1(8):e186040-0.

- 41 McCoy TH, Hughes MC. Preserving patient confidentiality as data grow: implications of the ability to reidentify physical activity data. *JAMA network open*. 2018;1(8):e186029-9.
- 815 42 Alam MAU. Person re-identification attack on wearable sensing. arXiv preprint arXiv:210611900. 2021.
- 43 Garfinkel S, et al.. De-identification of Personal Information... US Department of Commerce, National Institute of Standards and Technology; 2015.
- 820 44 CynergisTek R. BREACH REPORT 2016: Protected Health Information (PHI). February; 2017.
- 45 Li N, Li T, Venkatasubramanian S. t-closeness: Privacy beyond k-anonymity and l-diversity. In: 2007 IEEE 23rd international conference on data engineering. IEEE; 2006. p. 106-15.
- 825 46 Samarati P. Protecting respondents identities in microdata release. *IEEE transactions on Knowledge and Data Engineering*. 2001;13(6):1010-27.
- 47 Machanavajjhala A, Kifer D, Gehrke J, Venkitasubramaniam M. l-diversity: Privacy beyond k-anonymity. *Acm transactions on knowledge discovery from data (tkdd)*. 2007;1(1):3-es.
- 830 48 Pinchot J, Cellante D. Privacy concerns and data sharing habits of personal fitness information collected via activity trackers. *Journal of Information Systems Applied Research*. 2021;14(2):4-13.
- 49 Haley TD. Illusory privacy. *Ind LJ*. 2022;98:75.
- 50 Karanasiou AP, Kang S. My quantified self, my FitBit and I: The polymorphic concept of health data and the sharerâs dilemma. *Digital Culture & Society*. 2016;2(1):123-42.
- 835 51 Reidenberg JR, Bhatia J, Breaux TD, Norton TB. Ambiguity in privacy policies and the impact of regulation. *The Journal of Legal Studies*. 2016;45(S2):S163-90.
- 52 Dong Z, Wang L, Xie H, Xu G, Wang H. Privacy analysis of period tracking mobile apps in the post-roe v. wade era. In: Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering; 2022. p. 1-6.
- 840 53 Campanella ST. Menstrual and fertility tracking apps and the Post Roe v. Wade era. 2022.
- 54 Lewandowska M. The fall of Roe v Wade: the fight for abortion rights is universal. *British Medical Journal Publishing Group*; 2022.
- 55 Spector-Bagdady K, Mello MM. Protecting the privacy of reproductive health information after the fall of Roe v Wade. In: *JAMA Health Forum*. vol. 3. American Medical Association; 2022. p. e222656-6.
- 845 56 Ard B. Confidentiality and the problem of third parties: Protecting reader privacy in the age of intermediaries. *Yale JL & Tech*. 2013;16:1.
- 57 Lebanoff L, Liu F. Automatic detection of vague words and sentences in privacy policies. arXiv preprint arXiv:180806219. 2018.
- 58 McCarthy M. Experts warn on data security in health and fitness apps. *BMJ: British Medical Journal (Online)*. 2013;347.
- 850 59 Asay CD. Consumer information privacy and the problems (s) of third-party disclosures. *Nw J Tech & Intell Prop*. 2012;11:321.
- 60 Mohamed KS. An introduction to Bluetooth. In: *Bluetooth 5.0 modem design for IoT devices*. Springer International Publishing Cham; 2021. p. 1-32.
- 61 Jordan R, Abdallah CT. Wireless communications and networking: an overview. *IEEE Antennas and Propagation Magazine*. 2002;44(1):185-93.
- 62 Nicopolitidis P, Pomportsis A, Papadimitriou GI, Obaidat MS. *Wireless networks*. John Wiley & Sons, Inc.; 2003.

- 63 Maple C. Security and privacy in the internet of things. *Journal of cyber policy*. 2017;2(2):155-84.
- 64 Park YG, Lee S, Park JU. Recent progress in wireless sensors for wearable electronics. *Sensors*.
855 2019;19(20):4353.
- 65 Barua A, Al Alamin MA, Hossain MS, Hossain E. Security and privacy threats for bluetooth low energy in iot and
wearable devices: A comprehensive survey. *IEEE Open Journal of the Communications Society*. 2022;3:251-81.
- 66 Blow F, Hu YH, Hoppa M. A study on vulnerabilities and threats to wearable devices. In: *Journal of The
Colloquium for Information Systems Security Education*. vol. 7; 2020. p. 7-7.
- 67 Hale ML, Lotfy K, Gamble RF, Walter C, Lin J. Developing a platform to evaluate and assess the security of
wearable devices. *Digital Communications and Networks*. 2019;5(3):147-59.
860
- 68 Callaghan M, Harkin J, McGinnity T, et al. Case study on the Bluetooth vulnerabilities in mobile devices. *IJCSNS
International Journal of Computer Science and Network Security*. 2006;6(4):125-9.
- 69 Ryan M. Bluetooth: With low energy comes low security. In: *7th USENIX Workshop on offensive technologies
(WOOT 13)*; 2013..
865
- 70 Picco GP, Julien C, Murphy AL, Musolesi M, Roman GC. Software engineering for mobility: reflecting on the
past, peering into the future. In: *Future of Software Engineering Proceedings*; 2014. p. 13-28.
- 71 David Emm A. Kaspersky Security Bulletin 2015. Top security stories Retrieved from Kaspersky:
<https://securelist.com/kaspersky-security-bulletin-2015-top-security-stories/72886>. 2015.
870
- 72 Geevarghese D. Ble vs wi-fi: Which is better for iot product development. URL <https://www.cabotsolutions.com/ble-vs-wi-fi-which-is-better-for-iot-development>. 2018.
- 73 Woolf N. DDoS attack that disrupted internet was largest of its kind in history, experts say. *The Guardian*.
2016;26.
- 74 Lackner G. A Comparison of Security in Wireless Network Standards with a Focus on Bluetooth, WiFi and
WiMAX. *Int J Netw Secur*. 2013;15(6):420-36.
875
- 75 Zou Y, Zhu J, Wang X, Hanzo L. A survey on wireless security: Technical challenges, recent advances, and
future trends. *Proceedings of the IEEE*. 2016;104(9):1727-65.
- 76 Cichonski J, Franklin J, Bartock M. Guide to LTE security. National Institute of Standards and Technology;
2016.
- 77 Cäsar M, Pawelke T, Steffan J, Terhorst G. A survey on Bluetooth Low Energy security and privacy. *Computer
Networks*. 2022;205:108712.
880
- 78 Mahmood NQ, Culmone R. An ANT+ protocol based health care system. In: *2015 IEEE 29th International
Conference on Advanced Information Networking and Applications Workshops*. IEEE; 2015. p. 193-8.
- 79 Bhatti DS, Saleem S, Imran A, Iqbal Z, Alzahrani A, Kim H, et al. A survey on wireless wearable body area
networks: A perspective of technology and economy. *Sensors*. 2022;22(20):7722.
885
- 80 Abd Allah MM. Strengths and weaknesses of near field communication (NFC) technology. *Global Journal of
Computer Science and Technology*. 2011;11(3):51-6.
- 81 Rieback MR, Crispo B, Tanenbaum AS. Is your cat infected with a computer virus? In: *Fourth Annual IEEE
International Conference on Pervasive Computing and Communications (PERCOM'06)*. IEEE; 2006. p. 10-pp.
- 82 Lu HJ, Liu D. An improved NFC device authentication protocol. *Plos one*. 2021;16(8):e0256367.
890
- 83 Das AK, Zeadally S, He D. Taxonomy and analysis of security protocols for Internet of Things. *Future Generation
Computer Systems*. 2018;89:110-25.

- 84 Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A. Security, privacy and trust in Internet of Things: The road ahead. Computer networks. 2015;76:146-64.
- 895 85 Vanhoef M, Piessens F. Key reinstallation attacks: Forcing nonce reuse in WPA2. In: Proceedings of the 2017 ACM SIGSAC conference on computer and communications security; 2017. p. 1313-28.
- 86 Aldowah H, Ul Rehman S, Umar I. Security in internet of things: issues, challenges and solutions. In: Recent Trends in Data Science and Soft Computing: Proceedings of the 3rd International Conference of Reliable Information and Communication Technology (IRICT 2018). Springer; 2019. p. 396-405.
- 900 87 Koçi R, Franch X, Jovanovic P, Abelló A. A data-driven approach to measure the usability of web APIs. In: 2020 46th Euromicro Conference on Software Engineering and Advanced Applications (SEAA). IEEE; 2020. p. 64-71.
- 88 Lomborg S, Bechmann A. Using APIs for data collection on social media. The Information Society. 2014;30(4):256-65.
- 905 89 Fett D, Küsters R, Schmitz G. A comprehensive formal security analysis of OAuth 2.0. In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security; 2016. p. 1204-15.
- 90 90 Reschke J. The 'Basic' HTTP authentication scheme; 2015.
- 91 91 Shekh-Yusef R, Ahrens D, Bremer S. HTTP digest access authentication; 2015.
- 92 Heiland R, Koranda S, Marru S, Pierce M, Welch V. Authentication and authorization considerations for a multi-tenant service. In: Proceedings of the 1st Workshop on The Science of Cyberinfrastructure: Research, Experience, Applications and Models; 2015. p. 29-35.
- 910 93 Meli M, McNiece MR, Reaves B. How bad can it git? characterizing secret leakage in public github repositories. In: NDSS; 2019. .
- 94 Hammer-Lahav E. The oauth 1.0 protocol; 2010.
- 915 95 Hardt D. The OAuth 2.0 authorization framework; 2012.
- 96 Campbell B, Bradley J, Sakimura N, Lodderstedt T. OAuth 2.0 mutual-TLS client authentication and certificate-bound access tokens. Internet Requests for Comments, IETF, RFC 8705. 2020.
- 97 Li W, Mitchell CJ. User access privacy in OAuth 2.0 and OpenID connect. In: 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE; 2020. p. 664-6732.
- 920 98 Yu Y, Jatowt A, Doucet A, Sugiyama K, Yoshikawa M. Multi-timeline summarization (mtls): Improving timeline summarization by generating multiple summaries. In: Proceedings of the 59th Annual Meeting of the Association for Computational Linguistics and the 11th International Joint Conference on Natural Language Processing (Volume 1: Long Papers); 2021. p. 377-87.
- 99 Care AD. Privacy Policy; 2020. Accessed: 2024-11-29. Available from: <https://www.freestyleabbott/in-en/privacy-policy.html>.
- 925 100 Care AD. FreeStyle Libre 2 Continuous Glucose Monitoring System; 2024. Accessed: 2024-11-29. Available from: <https://www.freestyle.abbott/us-en/products/freestyle-libre-2.html>.
- 101 Britton KE, Britton-Colonnese JD. Privacy and Security Issues Surrounding the Protection of Data Generated by Continuous Glucose Monitors. Journal of Diabetes Science and Technology. 2017;11(2):216-9. Accessed: 2024-11-29. Available from: <https://doi.org/10.1177/1932296816681585>.
- 930 102 Care AD. Your Complete Guide; 2021. Accessed: 2024-11-29. Available from: https://www.freestylelibre.com.au/media/pdf-downloads/13367_FSL_Tips_Tricks_Booklet_Updated_A5_v7B.pdf.

- 103 ActiGraph. Privacy Policy; 2024. Accessed: 2024-11-29. Available from: <https://theactigraph.com/privacy-policy>.
- 935
104 Sweden TG. CenterPoint; Accessed: 2024-11-29. Available from: <https://timik.se/produkter/centerpoint/>.
- 105 ActiGraph. CentrePoint Insight Watch User Guide; 2020. Accessed: 2024-11-29. Available from: https://s3.amazonaws.com/actigraphcorp.com/wp-content/uploads/2020/03/05155854/ActiGraph_CPIW_UserGuide_E.200.6002_Revision4_FINAL.pdf.
- 940
106 ActiGraph. Center for Digital Health; 2024. Accessed: 2024-11-29. Available from: <https://actigraphcorp.com/cdh/>.
- 107 ActiGraph. CentrePoint (V3) API Documentation; 2024. Accessed: 2024-11-29. Available from: <https://github.com/actigraph/CentrePoint3APIDocumentation>.
- 945
108 Inc A. Intro to Health Data on iPhone; 2024. Accessed: 2024-11-29. Available from: <https://support.apple.com/guide/iphone/intro-to-health-data-iphbb8259c61/ios>.
- 109 Inc A. Apple Privacy Policy; 2024. Accessed: 2024-11-29. Available from: <https://www.apple.com/legal/privacy/en-ww/>.
- 950
110 Inc A. Differential Privacy Overview; 2017. Accessed: 2024-11-29. Available from: https://www.apple.com/privacy/docs/Differential_Privacy_Overview.pdf.
- 111 Esposito F. watchOS 9 adds new APIs for sharing and VoIP apps on Apple Watch; 2022. Accessed: 2024-11-29. Available from: <https://9to5mac.com/2022/06/08/watchos-9-apis-sharing-and-voip-apps/>.
- 955
112 Inc A. Connect your Apple Watch to Wi-Fi; 2024. Accessed: 2024-11-29. Available from: <https://support.apple.com/en-us/111818>.
- 113 Inc A. Intro to Health Data on iPhone; 2024. Accessed: 2024-11-29. Available from: <https://support.apple.com/guide/iphone/intro-to-health-data-iphbb8259c61/ios>.
- 114 Inc A. Track your nightly wrist temperature changes with Apple Watch; 2024. Accessed: 2024-11-29. Available from: <https://support.apple.com/en-us/102674>.
- 960
115 Inc A. Track your sleep on Apple Watch and use Sleep on iPhone; 2024. Accessed: 2024-11-29. Available from: <https://support.apple.com/en-us/108906>.
- 116 Inc A. Receive Retrospective Ovulation Estimates on Apple Watch; 2024. Accessed: 2024-11-29. Available from: <https://support.apple.com/en-us/120357>.
- 965
117 Inc A. Connect iPhone to the Internet; 2023. Accessed: 2024-11-29. Available from: <https://support.apple.com/guide/iphone/connect-to-the-internet-iphd1cf4268/ios>.
- 118 Inc A. HealthKit; 2024. Accessed: 2024-11-29. Available from: <https://developer.apple.com/documentation/healthkit>.
- 970
119 Fullerton SM, Lee SSJ. Secondary Uses and the Governance of De-Identified Data: Lessons from the Human Genome Diversity Panel. *The American Journal of Bioethics*. 2010;10(9):3-11. Accessed: 2024-11-29. Available from: <https://doi.org/10.1080/15265161.2010.494215>.
- 120 Levey S, Levey T, Fligor BJ. Noise Exposure Estimates of Urban MP3 Player Users. *Journal of Speech, Language, and Hearing Research*. 2011;54(1):263-77. Accessed: 2024-11-29. Available from: [https://doi.org/10.1044/1092-4388\(2010/09-0283\)](https://doi.org/10.1044/1092-4388(2010/09-0283)).
- 975
121 Huckvale K, Torous J, Larsen ME. Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation. *JAMA Network Open*. 2019;2(4):e192542. Accessed: 2024-11-29. Available from: <https://doi.org/10.1001/jamanetworkopen.2019.2542>.

- 122 Inc A. Set up your Medical ID in the Health app on your iPhone; 2024. Accessed: 2024-11-29. Available from: <https://support.apple.com/en-us/105072>.
- 123 Inc A. Make an emergency call from a locked iPhone; 2024. Accessed: 2024-11-29. Available from: <https://support.apple.com/en-us/102262>.
- 980 124 Inc A. Use the Health app on your iPhone or iPad; 2024. Accessed: 2024-11-29. Available from: <https://support.apple.com/en-us/104997>.
- 125 Inc A. Encryption and Data Protection Overview; 2020. Accessed: 2024-11-29. Available from: <https://support.apple.com/guide/security/encryption-and-data-protection-overview-sece3bee0835/1/web/1>.
- 985 126 Inc A. Apple Platform Security; 2024. Accessed: 2024-11-29. Available from: https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf.
- 127 Inc A. Apple Advertising & Privacy; 2024. Accessed: 2024-11-29. Available from: <https://www.apple.com/legal/privacy/data/en/apple-advertising/>.
- 990 128 COROS. COROS Privacy Policy; 2022. Archived version available at: <https://web.archive.org/web/20221209021601/https://coros.com/privacy>. Available from: <https://coros.com/privacy>.
- 129 COROS. How to Connect Your COROS Device with Your Phone and the COROS App; 2024. Accessed: 2024-11-29. Available from: <https://support.coros.com/hc/en-us/articles/360039835692-How-to-connect-your-COROS-device-with-your-phone-and-the-COROS-app>.
- 995 130 Dexcom. How Does Dexcom G6 Pro CGM Work?; 2024. Accessed: 2024-11-29. Available from: <https://provider.dexcom.com/products/dexcom-g6-pro/how-it-works>.
- 131 Dexcom. Privacy Policy; 2024. Accessed: 2024-11-29. Available from: <https://www.dexcom.com/linked/documentservice/PrivacyPolicy>.
- 1000 132 Dexcom. What are the recommended G6 iPhone settings?; 2024. Accessed: 2024-11-29. Available from: <https://www.dexcom.com/en-IE/faqs/what-are-recommended-g6-iphone-settings>.
- 133 Dexcom. Authentication; 2024. Accessed: 2024-11-29. Available from: <https://developer.dexcom.com/docs/dexcom/authentication>.
- 1005 134 Fitbit. Fitbit Privacy Policy; 2024. Accessed: 2024-11-29. Available from: <https://www.fitbit.com/global/us/legal/privacy-policy>.
- 135 Fitbit. How do I set up my Fitbit device?; 2024. Accessed: 2024-11-29. Available from: <https://support.google.com/fitbit/answer/14236818>.
- 136 Fitbit. Authorization; Accessed: 2024-11-29. Available from: <https://dev.fitbit.com/build/reference/web-api/authorization>.
- 1010 137 Ltd G. Garmin Connect Privacy Policy; 2024. Accessed: 2024-11-29. Available from: <https://www.garmin.com/en-US/privacy/connect/policy/>.
- 138 Shilton K. Four Billion Little Brothers? Privacy, Mobile Phones, and Ubiquitous Data Collection. Communications of the ACM. 2009;52(11):48-53. Accessed: 2024-11-29. Available from: <https://doi.org/10.1145/1592761.1592778>.
- 1015 139 Torous J, Baker J, Keshavan LS, Keshavan MS. Self-Monitoring and Routines in Bipolar Disorder: A Smartphone Pilot Study. Journal of the American Medical Informatics Association. 2016;23(3):477-83. Accessed: 2024-11-29. Available from: <https://doi.org/10.1093/jamia/ocv165>.

- 140 Kay M, Choe EK, Jung J, Harrison BL, Patel SN, Kientz JA. Lullaby: A Capture & Access System for Understanding the Sleep Environment. In: Proceedings of the 2012 ACM Conference on Ubiquitous Computing; 2012. p. 226-35. Accessed: 2024-11-29. Available from: <https://doi.org/10.1145/2370216.2370253>.
- 1020 141 Ltd G. Garmin Global Privacy Policy; 2023. Accessed: 2024-11-29. Available from: <https://www.garmin.com/en-US/privacy/global/policy/>.
- 142 Ltd G. California Privacy Notice; 2023. Accessed: 2024-11-29. Available from: <https://www.garmin.com/en-US/privacy/ccpa/policy/>.
- 1025 143 Newman LH. A Cyberattack on Garmin Disrupted More Than Workouts; 2020. Accessed: 2024-11-29. Available from: <https://www.wired.com/story/garmin-outage-ransomware-attack-workouts-aviation/>.
- 144 Ltd G. fÄnix® 7 Standard/Solar/Pro Series Owner's Manual; 2024. Accessed: 2024-11-29. Available from: <https://www8.garmin.com/manuals/webhelp/GUID-C001C335-A8EC-4A41-AB0E-BAC434259F92/EN-US/GUID-A320BB2B-B192-4CDF-931E-52FC01144D1E.html>.
- 1030 145 Ltd G. Module: Toybox.Authentication; 2024. Accessed: 2024-11-29. Available from: <https://developer.garmin.com/connect-iq/api-docs/Toybox/Authentication.html>.
- 146 Nutrisense I. Nutrisense Privacy Policy; 2024. Accessed: 2024-11-29. Available from: <https://www.nutrisense.io/privacy-policy>.
- 1035 147 Wearipedia. Abbott Freestyle Libre CGM: Guide to Data Extraction and Analysis; 2022. Accessed: 2024-11-29. Available from: https://wearipedia.readthedocs.io/en/stable/notebooks/nutrisense_cgm.html.
- 148 Oy OH. Oura API Documentation; 2024. Accessed: 2024-11-29. Available from: <https://cloud.ouraring.com/docs>.
- 1040 149 Oy OH. Oura API Documentation V2; 2024. Accessed: 2024-11-29. Available from: <https://cloud.ouraring.com/v2/docs>.
- 150 Oy OH. How Oura Protects Your Data; 2024. Accessed: 2024-11-29. Available from: <https://support.ouraring.com/hc/en-us/articles/360025586673-How-Oura-Protects-Your-Data>.
- 1045 151 Oy OH. Oura Health Privacy Policy; 2024. Accessed: 2024-11-29. Available from: <https://ouraring.com/privacy-policy-oura-health>.
- 152 Oy OH. Set Up an Oura Ring; 2024. Accessed: 2024-11-29. Available from: <https://support.ouraring.com/hc/en-us/articles/4411128662291-Set-Up-an-Oura-Ring>.
- 1050 153 Oy OH. Set Up the Oura App; 2024. Accessed: 2024-11-29. Available from: <https://support.ouraring.com/hc/en-us/articles/360058634153-Set-Up-the-Oura-App>.
- 154 Oy OH. Authentication; 2023. Accessed: 2024-11-29. Available from: <https://cloud.ouraring.com/docs/authentication>.
- 155 Electro P. Privacy FAQ; 2024. Accessed: 2024-11-29. Available from: <https://www.polar.com/en/legal/faq>.
- 1055 156 Electro P. Polar H10 Heart Rate Sensor; 2024. Accessed: 2024-11-29. Available from: <https://www.polar.com/us-en/sensors/h10-heart-rate-sensor>.
- 157 Electro P. Polar AccessLink API Documentation; 2024. Accessed: 2024-11-29. Available from: <https://www.polar.com/accesslink-api/#authentication>.

- 158 Electro P. Polar Vantage V2 User Manual: Technical Specifications; 2024. Accessed: 2024-
1060 11-29. Available from: https://support.polar.com/e_manuals/vantage-v2/polar-vantage-v2-user-manual-english/technical-specifications.htm.
- 159 Electro P. Polar Vantage M2 User Manual; 2023. Accessed: 2024-11-29. Available from: https://support.polar.com/e_manuals/vantage-m2/polar-vantage-m2-user-manual-english/manual.pdf.
- 1065 160 Electro P. Polar Verity Sense User Manual; 2024. Accessed: 2024-11-29. Available from: https://support.polar.com/e_manuals/verity-sense/polar-verity-sense-user-manual-english/manual.pdf.
- 161 Electro P. Polar Verity Sense; 2024. Accessed: 2024-11-29. Available from: <https://www.polar.com/en/products/accessories/polar-verity-sense>.
- 1070 162 SLEEPON. Privacy Policy of SLEEPON; 2024. Accessed: 2024-11-29. Available from: <https://www.sleepon.us/privacy/>.
- 163 SLEEPON. SLEEPON Official Website; 2024. Accessed: 2024-11-29. Available from: <https://www.sleepon.us/home/>.
- 1075 164 Suunto. Suunto 7 User Guide: Daily Activity; 2024. Accessed: 2024-11-29. Available from: https://www.suunto.com/Support/Product-support/suunto_7/suunto_7/activity-tracking/.
- 165 Suunto. Suunto Customer Privacy Policy; 2024. Accessed: 2024-11-29. Available from: <https://www.suunto.com/Privacy-Policy/>.
- 166 Suunto. Suunto Smart Heart Rate Belt; 2024. Accessed: 2024-11-29. Available from: <https://www.suunto.com/Products/Heart-Rate-Belts/suunto-smart-heart-rate-belt/>.
- 1080 167 Suunto. Suunto API Zone Services Documentation; 2024. Accessed: 2024-11-29. Available from: <https://apizone.suunto.com/docs/services>.
- 168 WHOOP. WHOOP API Documentation; 2024. Accessed: 4 November 2024. Available from: <https://developer.whoop.com/api/>.
- 1085 169 WHOOP. WHOOP Full Privacy Policy; 2023. Accessed: 2024-11-29. Available from: <https://www.whoop.com/privacy/full-privacy-policy/>.
- 170 Murnane EL, Matthews M, Kay MH, Choudhury T, Gay G. Self-monitoring practices, attitudes, and needs of individuals with bipolar disorder: implications for the design of technologies to support mental health. Journal of the American Medical Informatics Association. 2016;23(3):477-84. Available from: <https://doi.org/10.1093/jamia/ocv165>.
- 1090 171 WHOOP. Connectivity FAQ: Commonly Asked Questions; 2022. Accessed: 2024-11-29. Available from: https://support.whoop.com/Connectivity/Commonly_Asked_Questions/Why_is_my_WHOOP_%22Catching_Up%22.
- 172 WHOOP. "Data Catching Up" - Android; 2022. Accessed: 2024-11-29. Available from: https://support.whoop.com/Connectivity/WHOOP_3.0_-_Android/%22Data_Catching_Up%22_-_Android.
- 1095 173 Withings. Withings Privacy Policy; 2024. Accessed: 2024-11-29. Available from: <https://www.withings.com/us/en/legal/privacy-policy>.
- 174 Withings. Body+ - Updating the Body+ Communication Mode (Wi-Fi Network or Bluetooth); 2024. Accessed: 2024-11-29. Available from: <https://support.withings.com/hc/en-us/articles/219053097-Body-Updating-the-Body-communication-mode-Wi-Fi-Network-or-Bluetooth>.

- 175 Withings. OAuth Web Flow; 2024. Accessed: 2024-11-29. Available from: <https://developer.withings.com/developer-guide/v3/integration-guide/public-health-data-api/get-access/oauth-web-flow/>.
- 176 Withings. ScanWatch: Hybrid Smartwatch - ECG, Heart Rate Sensor and Oximeter Installation and Operating Instructions; 2023. Accessed: 2024-11-29. Available from: https://support.withings.com/hc/article_attachments/13743798632977.
- 177 Withings. ScanWatch - Installing My Device; 2024. Accessed: 2024-11-29. Available from: <https://support.withings.com/hc/en-us/articles/360009852557-ScanWatch-Installing-my-device>.
- 178 Withings. Withings API Reference; 2024. Accessed: 2024-11-29. Available from: <https://developer.withings.com/api-reference/>.
- 179 Withings. Sleep (U.S.) - Does my device emit Bluetooth or Wi-Fi signals while I sleep?; 2024. Accessed: 2024-11-29. Available from: <https://support.withings.com/hc/en-us/articles/4411175659793-Sleep-U-S-Does-my-device-emit-Bluetooth-or-Wi-Fi-signals-while-I-sleep->.
- 180 Cronometer. Privacy Policy; 2024. Accessed: 2024-11-29. Available from: <https://cronometer.com/privacy>.
- 181 MyFitnessPal. MyFitnessPal Privacy Policy; 2020. Accessed: 2024-11-29. Available from: <https://www.myfitnesspal.com/privacy-policy>.
- 182 MyFitnessPal. MyFitnessPal API User Authentication; 2024. Accessed: 2024-11-29. Available from: <https://myfitnesspalapi.com/docs/user-authentication/>.
- 183 Strava. Strava Privacy Policy; 2024. Accessed: 2024-11-29. Available from: <https://www.strava.com/legal/privacy>.
- 184 Strava. Strava API Authentication; 2024. Accessed: 2024-11-29. Available from: <https://developers.strava.com/docs/authentication/>.