Vesselkov, Alexandr; Hämmäinen, Heikki; Töyli, Juuso

**Design and governance of mHealth data sharing**

*Published in:*
Communications of the Association for Information Systems

*DOI:*
10.17705/1CAIS.04518

Published: 01/01/2019

*Document Version*
Publisher's PDF, also known as Version of record

*Please cite the original version:*
Vesselkov, A., Hämmäinen, H., & Töyli, J. (2019). Design and governance of mHealth data sharing. *Communications of the Association for Information Systems* , *45*, 299-321. Article 18.
https://doi.org/10.17705/1CAIS.04518

Communications of the Association for Information Systems

Volume 45 Article 18

10-2019

# Design and Governance of mHealth Data Sharing

Alexandr Vesselkov
*Aalto University*, alexandr.vesselkov@aalto.fi

Heikki Hämmäinen
*Aalto University*

Juuso Töyli
*University of Turku*

Communications of the Association for Information Systems

Research Paper DOI: 10.17705/1CAIS.04518 ISSN: 1529-3181

# Design and Governance of mHealth Data Sharing

**Alexandr Vesselkov**
Department of Communications and Networking
Aalto University
*alexandr.vesselkov@aalto.fi*

**Heikki Hämmäinen**
Department of Communications and Networking
Aalto University

**Juuso Töyli**
Turku School of Economics
University of Turku,
Department of Communications and Networking
Aalto University

## Abstract:

The proliferation of mobile health (mHealth)—namely, mobile applications along with wearable and digital health devices—has helped to generate a growing amount of heterogeneous data. To increase devices' and apps' value via facilitating new ways to use data, mHealth companies often provide a Web application programming interface (API) to their cloud data repositories, which enables third-party developers to access end users' data after receiving their consent. Managing such data sharing requires making design and governance decisions that maintain the tradeoff between promoting generativity to facilitate complementors' contributions and retaining control to prevent undesirable platform use. However, despite the increasing pervasiveness of Web data-sharing platforms, researchers have not sufficiently analyzed their design and governance. By relying on boundary resource theory and analyzing documents about 21 Web data-sharing platforms, we identify and 18 design and governance decisions that mHealth companies must make to manage data sharing and discuss their role in maintaining the tradeoff between platform generativity and control.

**Keywords:** Data Sharing, Web Platform, Boundary Resources, Generativity and Control, Data Economy.

This manuscript underwent peer review. It was received 03/22/2018 and was with the authors for 4 months for 3 revisions. Ali Sunyaev served as Associate Editor.

# 1 Introduction

Wearable devices have become more numerous, accurate, diverse, and affordable. In turn, these devices have led to an increasing amount of heterogeneous health and fitness data. Wearable producers typically provide an accompanying mobile app and Web service that allows users to analyze and interpret the data their devices generate. However, due to constraints associated with available resources and application scope, device producers use data in a limited number of ways. Therefore, to increase the value and sales of their hardware products and to create new applications, wearable manufacturers often open an application programming interface (API) to their data repository. Such a public Web API turns a Web data repository into a data-sharing platform that, with end users' consent, enables third-party innovators to access end users' data that wearable producers manage (Grundy, Held, & Bero, 2017).

Data sharing[1] holds many potential advantages for data consumers, providers, and their end users, which explains the growing number of data-sharing integrations in mobile health (mHealth) (Research2guidance, 2016). Mobile health refers to the field that uses mobile applications and devices, which includes wearables, to help users achieve health, wellness, and fitness targets (Olla & Shimskey, 2015). However, open data sharing may challenge a data provider's (e.g., a wearable device producer or another mHealth company) competitive position because its end-user service often relies on the shared data. Data providers can decrease such competitive risks by setting up restrictions and limitations on the data use, which, however, discourage third parties from collaborating.

Data providers and consumers typically share mobile health data through platforms. Therefore, we can view the problem of facilitating third-party developers' innovativeness while restricting their undesirable actions in a platform-design and governance context. Indeed, to attract a sufficient number of platform complementors (i.e., supply-side users), platform providers must enhance platform generativity that determines how easily complementors can leverage a platform to develop and provide services (Zittrain, 2008). At the same time, a platform provider must define technical and business conditions that would govern how the complementors can use the platform and facilitate platform control. Maintaining the tradeoff between promoting generativity and keeping control represents a critical task in designing and governing platforms (Eaton, Elaluf-Calderwood, Sørensen, & Yoo, 2011; Förderer, Kude, Schütz, & Heinzl, 2014). However, research has not sufficiently analyzed this topic for increasingly ubiquitous data-sharing platforms in general and mHealth data-sharing platforms in particular. Similarly, the more general literature on platform design and governance has scarcely and disjointedly analyzed the topic (Manner, Nienaber, Schermann, & Krcmar, 2013; Tiwana, Konsynski, & Bush, 2010), and most studies have primarily focused on large-scale marketplaces or mobile application platforms, such as the Apple's App Store (e.g., Ghazawneh & Henfridsson, 2013), Google Play, and Alibaba (e.g., Hein, Schreieck, Wiesche, & Krcmar, 2016). Such cases differ from the ones in mHealth not only in the opened resource type but also in platform size and architecture; thus, they potentially require different governance mechanisms (Tiwana, 2013). Furthermore, previous studies have not paid sufficient attention to the role of platform design and governance as means to reduce competition with complementors—a significant risk in mHealth because data providers and consumers serve the same end users relying on the overlapping (shared) data. Finally, mHealth differs from other analyzed platforms in that it deals with a highly sensitive resource—user data—which potentially demands special governance mechanisms. Therefore, motivated by the growing interconnection between mHealth applications and the scarcity of literature on designing and governing data platforms[2], we examine the following research question:

> **RQ:** What design and governance decisions must mHealth companies make to manage Web mHealth data sharing?

Recently, Ghazawneh and Henfridsson (2013) conceptualized boundary resources as tools for managing platforms and stimulating their generativity while keeping control. Boundary resources include technical and non-technical tools, such as APIs and developer terms agreements, which enable platform providers to maintain an arm's length relationship with third-party developers. Therefore, we analyzed boundary resources to answer our research question. To identify the case platforms to analyze, we selected 37 mHealth companies most actively participating in data sharing, identified 192 integrations between them, and inspected these integrations to detect platforms that enabled data sharing. By doing so, we could also explore the mHealth data-sharing ecosystem and identify participating mHealth companies' roles. Further,

[1] "Data sharing" refers to both providing and using (consuming) provided data.
[2] Hereafter, we use "data platform" and "data-sharing platform" interchangeably.

we collected and analyzed boundary resource documents (API references and developers' terms) for the detected 21 web mHealth data-sharing platforms with openly available documentation to identify design and governance decisions that they used to manage data sharing.

Synthesizing the design and governance decisions that platform providers have made for their existing mHealth data platforms can help strategic planners in entering the mHealth data-sharing ecosystem. Platform providers can use the defined decisions as levers to affect platform generativity and control. Further, researchers can use our results as a foundation for further explanatory analyses, such as to investigate the impact that each decision has on platform use in quantitative terms. Apart from mHealth industry, our results may also assist other domains in consumer Internet of things (IoT) and beyond where different parties share sensitive data and where sharing can potentially lead to competition between a data provider and complementor. Finally, by serving as an early example for examining how platform providers design and govern platforms to share data in the private sector, our study contributes to both the platform and data-sharing literatures.

This paper proceeds as follows: in Section 2, we present the background literature on APIs and platformization, platform design and governance, and data sharing and examine the current state of mHealth data sharing. In Section 3, we describe our research approach and selected cases. In Section 4, we present and examine the design and governance decisions that platform providers have made for sharing mHealth data. In Section 5, we discuss the impact that these decisions have on generativity and control and present challenges in designing and governing data sharing in mHealth. Finally, in Section 6, we conclude the paper.

# 2 Background

## 2.1 Platformization and Platform Types

An application programming interface (API) constitutes a means to allow third parties to access an organization's capabilities or data (Spencer, Krohn, Fisher, & Boyd, 2014). External APIs act as platform boundary resources: "the software tools and regulations that serve as the interface for the arm's-length relationship between the platform owner and the application developer" (Ghazawneh & Henfridsson, 2013, p. 175). Therefore, external APIs drive product "platformization" (Helmond, 2015)—the process of making a platform from a non-platform good (Patel, 2015). In turn, information systems (IS) research typically understands a platform as an extensible software-based system with core functionality that modules that interoperate with it share (Tiwana et al., 2010). However, economists define a (multi-sided) platform as a market that enables direct interactions between several groups of users who make investments to affiliate with the platform and provide each other with network benefits (Hagiu & Wright, 2015). Although some platforms, such as Android OS, may comply with both definitions, some others meet only one. Thus, Airbnb represents a multi-sided (two-sided) market platform that lacks a platform's features in an IS sense, whereas many IoT middleware solutions, such as Kaa[3], that focus on simplifying IoT application development do not have a marketplace of third-party applications (Mineraud, Mazhelis, Su, & Tarkoma, 2016) and, therefore, do not create a multi-sided market.

One can categorize external APIs into three levels (Andreessen, 2007), which can serve as a basis for classifying platforms that public APIs enable. The first level, "access API", allows external developers to access platforms' data and capabilities by making calls—typically via protocols such as REST or SOAP. At the same time, developers' applications reside outside the platforms. Fitbit API and the APIs of most other mHealth data platforms, which allow one to access platforms, exemplify access APIs. The second level, "plug-in API", allows developers to "plug in" the functions they build into core platforms, although the application's code runs outside the platforms. Browser plug-ins and extensions exemplify such APIs. Finally, the third level, "runtime environment API", allows third-party applications to run on platforms themselves. An example includes Salesforce APIs (Helmond, 2015).

## 2.2 Platform Design and Governance

When designing platforms, designers must provide sufficient means and motivation for third-party developers (complementors) to join while ensuring that platform providers and complementors can create and capture value efficiently by imposing rules regulating participants' behavior. Importantly, such rules

[3] https://www.kaaproject.org/overview/

should not limit complementors' creativity and platform generativity (Wareham, Fox, & Cano Giner, 2014), which refers to "a system's capacity to produce unanticipated change through unfiltered contributions from broad and varied audiences" (Zittrain, 2008, p.70). System generativity involves five factors: leverage, adaptability, ease of mastery, accessibility, and transferability (Tilson, Sorensen, & Lyytinen, 2013; Zittrain, 2008). *Leverage* defines how well the system allows complementors to perform a certain task, *adaptability* determines how easily one can build on the system for a wide range of uses, *ease of mastery* refers to how easily one can learn to use the system, *accessibility* refers to the system's openness and cost, and *transferability* determines the ease with which system users can transfer changes to other system users.

Supporting generativity while keeping control represents a key challenge in designing and governing platforms (Constantinides, Henfridsson, & Parker, 2018; Eaton et al., 2011; Tiwana et al., 2010; Yoo, Boland, Lyytinen, & Majchrzak, 2012). In order to resolve this tradeoff, platform providers must carefully design the platform API and other boundary resources. Such resources, which can be technical (API) and social (guidelines and agreements) (Ghazawneh, 2012), play a two-fold role: platform resourcing (enhancing diversity) and securing (Ghazawneh & Henfridsson, 2013), which makes them essential for managing the tradeoff that we discuss above. Therefore, the platform provider's decisions on designing boundary resources bear strategic importance (Yoo, Henfridsson, & Lyytinen, 2010).

The literature on platform design and governance remains scarce and fragmented (Manner et al., 2013; Tiwana et al., 2010). Moreover, existing studies seem to focus on mobile application platforms and, in particular, Apple. For example, Ghazawneh and Henfridsson (2013) used the boundary resource model to analyze the actions Apple took to enhance the diversity of its platform while retaining control. Eaton et al. (2015) similarly focused on Apple to show how third-party developers affected how platform boundary resources evolved and, therefore, how Apple governed it. Apart from Apple, Manner et al. (2013) considered Google's and Microsoft's mobile application platforms. Furthermore, to more comprehensively understand platform governance, Hein et al. (2016) analyzed different types of multi-sided platforms: social networks (Facebook), merchants (Alibaba), service platforms (Airbnb and Uber), and application platforms (Google Play Store and Apple App Store). However, even they did not consider data-sharing platforms, although governing such platforms may differ from other cases for several reasons. For example, data providers typically open data they use in their end-user service for sharing. Furthermore, services that data-consuming complementors provide can resemble the provider's services, which can lead the data consumer's service to substitute rather than complement the data provider's end-user service and, thereby, create a risk that platform providers need to resolve. Furthermore, no existing studies seem to have focused explicitly on platforms that rely on access APIs (Section 2.1). The difference in the platform API level (e.g., third level in Apple platform vs. first level in mHealth data-sharing platforms) may mean previous results have limited applicability because platform governance often relates to the platform architecture (Tiwana, 2013). With this study, we contribute to fulfilling these gaps. As such, our work represents an early effort into analyzing how platform providers design and govern platforms—which rely on access APIs—for sharing data (and mHealth data in particular).

Researchers have recently proposed several conceptual frameworks of platform design and governance. Tiwana (2013) defined platform governance as a three-dimensional concept that includes pricing policies, a division of decision rights and responsibilities between the platform owner and participants, and control mechanisms. Economists have largely focused on the first dimension—that is, pricing (Eisenmann, Parker, & Van Alstyne, 2006)—and often ignored the other two. Tura, Kutvonen, and Ritala (2017) proposed a platform design framework with four elements: architecture, value creation logic, competition, and governance. Schreieck, Wiesche, and Krcmar (2016) identified the most studied design and governance concepts in the platform literature: roles, pricing, openness, and boundary resources. Because these frameworks are general in nature and describe high-level elements of platform design and governance, they can serve as a starting point for analyzing mHealth data-sharing platforms. However, given that no existing framework focuses particularly on data-sharing platforms, we adopted an inductive approach to analyze a platform's boundary resources and, thus, determine specific design and governance decisions that platform providers make for mHealth data-sharing. In doing so, we ensured that we drew conclusions from the data rather than limiting our attention to pre-defined concepts.

## 2.3 Data Sharing

Data sharing can allow organizations to access complementary data sources and help them develop innovative applications and services. Actors in the public domain have long recognized data sharing's potential. Indeed, "open data", which refers to publicly funded data that mainly governmental organizations make available under non-restrictive conditions to enable innovative use cases, emerged from the public domain (Attard, Orlandi, Scerri, & Auer, 2015; Janssen, Charalabidis, & Zuiderwijk, 2012). However, data sharing in the public domain does not pose the same governance-related challenges as in the private domain (Eckartz, Hofman, & Van Veenstra, 2014). Therefore, the literature on open data does not typically address governance-related issues and cannot help one in designing and governing mHealth data sharing.

Health information exchange (HIE) between different healthcare institutions, which primarily focuses on maintaining continuity of care, represents another government-driven data-sharing initiative. In some countries with a private healthcare system, healthcare institutions compete with each other and, therefore, may not wish to share data. Such "overprotectiveness" and various legal issues represent primary governance challenges in HIE in the United States (Allen et al., 2014). Although market- and data sensitivity-related challenges commonly arise in both HIE and mHealth data sharing, their design and governance differ. For instance, multiple organizations typically collaboratively govern HIE (Vest & Gamm, 2010), whereas individual platform providers usually govern mHealth data sharing. Furthermore, HIE platforms must often adhere to stricter legal and technical requirements (e.g., Mello, Adler-Milstein, Ding, & Savage, 2018), whereas mHealth companies have more freedom in designing and governing data sharing.

In the private domain, trusted partners mostly share data based on a bilateral agreement to minimize competition-related risks, such as in logistics and supply chain management (e.g., Lee & Whang, 2000). Open data sharing through public APIs remains less established, although the Web's ubiquitous platformization has led some websites, notably social networks, to become data-sharing platforms. Thus, in 2006, Facebook introduced a Web API that enabled developers to bring users' data into external applications and, thereby, turned into a data-sharing platform (Helmond, 2015). However, although researchers often use such platforms and APIs to collect data, little research on them exists (Bucher, 2013). Studies that have specifically examined data-sharing platforms and APIs have often focused on the privacy and security concerns that personal data sharing may raise (e.g., Bodle, 2011; Puschmann & Burgess, 2014). Few studies seem to have addressed data sharing's design and governance perspectives. Thus, Bucher (2013) investigated the Twitter ecosystem and briefly discussed how the platform provider governed its relations with third-party developers from the developers' perspective. However, the author only analyzed the regulating role of API conceptually and did not define mechanisms that platform provides use to manage data sharing. Furthermore, Facebook and Twitter, which researchers have typically studied as data-sharing platforms, have a dominant role, which does not always apply for mHealth data sharing where complementors and platform providers may equal each other in size, which increases the competitive risks they experience from sharing data.

Finally, only a few studies have focused specifically on data sharing in mHealth. For instance, de Arriba-Pérez, Caeiro-Rodríguez, and Santos-Gago (2016) identified four different mHealth data-sharing approaches: 1) direct sensor, 2) indirect sensor, 3) direct warehouse, 4) indirect warehouse. In direct sharing, a third party receives the data to its cloud directly from a sensor or warehouse (cloud). In indirect sharing, a sensor or warehouse requires some intermediary system or gateway (e.g., a smartphone) to send data to the third party. The authors found that differences in data-sharing approaches and data models hinder mHealth's interoperability and development. Further, in a descriptive study in which they examined an mHealth data-sharing ecosystem, Grundy et al. (2017) conducted a network analysis of data-sharing links between mHealth apps and identified apps that had a central position in the ecosystem. They found that a highly interconnected market causes considerable privacy and security concerns.

Overall, open (as opposed to bilateral agreement-based) data sharing in the private domain constitutes a relatively new development; therefore, the literature on designing and governing such data sharing remains scarce, especially in cases where data sharing may challenge platform providers' and complementors' competitive position as in mHealth data sharing. Therefore, we contribute to filling this gap in this paper by analyzing how platform providers design and govern open data sharing in mHealth.

### 2.4 Current State of Data Sharing in mHealth

As an industry, mobile health continues to grow: in 2017, app stores contained 325,000 health, fitness, and medical apps—78,000 more than in 2016 (Research2guidance, 2017). To increase the customer base and engagement, mHealth companies use APIs to enable developers to share collected data with other developers. In 2016, 58 percent of mHealth developers participated in data sharing compared with 42 percent in 2015 (Research2guidance, 2016), which makes mHealth an advanced market in the API economy. Until recently, organizations predominantly shared mHealth data through peer-to-peer (P2P) API integrations. However, in 2014, Apple and Google launched their mHealth data-aggregating platforms Apple Health and Google Fit, respectively, to provide a central place for storing scattered mHealth data and facilitate data sharing by eliminating the need for non-scalable P2P integrations. The architectures of Apple's and Google's platforms significantly differ. While Google stores mHealth data in a cloud repository, Apple keeps the data locally on a device: iPhone or Apple Watch. Apart from their data-sharing capability, both Apple and Google provide developers with tools to access mobile devices' sensors. As a result, data sharing through hub platforms has significantly increased, although P2P connections to proprietary platforms account for a large part of mHealth data-sharing integrations (Research2guidance, 2016).

## 3 Research Approach and Cases

### 3.1 Case Selection

To determine the design and governance decisions that mHealth companies make to manage Web mHealth data sharing, we focused on identifying the mHealth data-sharing ecosystem's most active applications and services rather than mapping the ecosystem in its entirety. We considered data sharing as either third parties' opening the data they own or their consuming the data from other providers. We also considered only data-generating device producers that could control data sharing. Thus, we excluded, for example, smartwatches that run on Wear OS, which have raw sensor data that third parties can access through an API as a part of OS functionality and Bluetooth sensors that broadcast data in a standardized open format following General Attributes (GATT) profile specifications.

We summarize the logic we used to select relevant applications and services in Figure 1. We first picked the apps that had a central position in mHealth data-sharing landscape according to Grundy et al. (2017): MyFitnessPal, MapMyFitness/Run, Endomondo, RunKeeper, Lose It!, HealthMate (Nokia), Jawbone UP, Lifesum, Samsung Health, Strava, Apple HealthKit, Fitbit, and Runtastic. We excluded some non-mHealth apps, such as Facebook and Twitter, even though they connect to many mHealth services.

Then, based on an industry report (research2guidance, 2016), we added leading data and API aggregation services: Google Fit, Validic, and Human API[4]. After that, by browsing the directories of partners that the selected 16 services shared data with, we identified apps connected to each app and service we initially selected and additionally picked those ones that shared data with at least three of them. In some cases, partner listings were missing or incomplete; however, we used the best available information. After reviewing the picked apps, we omitted some due to their either inactivity (no app version updates for more than a year, such as EveryMove) or our inability to validate the existence of connections[5]. Overall, in addition to the initially selected 16 apps and services, we added 21 more, which resulted in 37 in total (see Appendix A).

From the 37 apps and services we selected, we removed ones that did not share data through their own proprietary API (Figure 1), which left 26 apps and services. Subsequently, we removed five apps and services that did not have publicly available documentation for their APIs. Furthermore, to ensure the comparability of cases, we selected only Web APIs since they constitute the prevailing way to share data. As a result, we obtained 19 apps and services and 20 APIs (Validic had two Web APIs). Finally, we added two more platform APIs (Dexcom and PredictBG) to account for medical (rather than pure fitness) apps and services to ensure we analyzed diverse mHealth data-sharing platforms. Thus, we ended up 21 apps and services and 22 APIs in total (see Table A1).

[4] We excluded Open Health due to negative dynamics in the share of mHealth developers using it.

[5] We could not verify Validic's and Human API's connections because they operated only in business-to-business (B2B) segment. However, we included all connections that their websites listed.

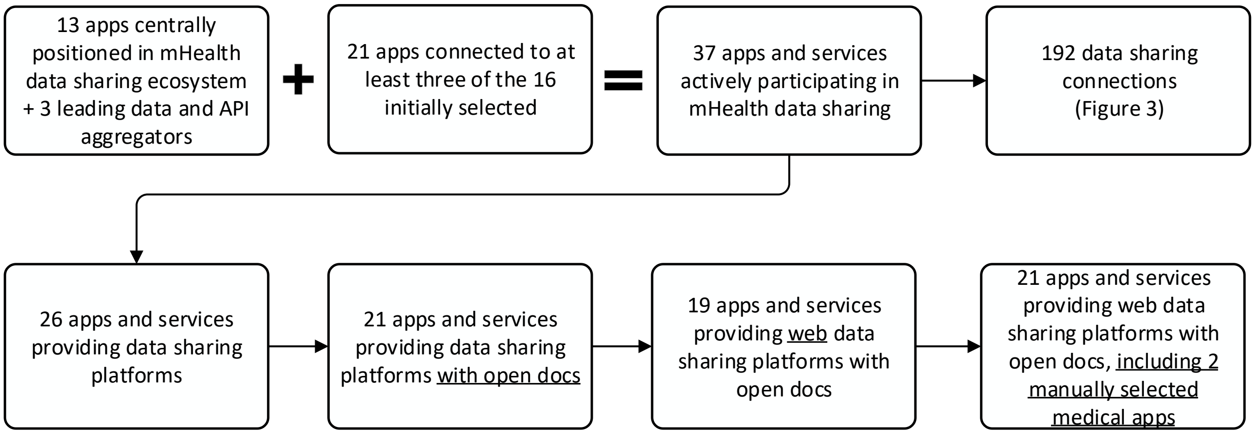
13 apps centrally positioned in mHealth data sharing ecosystem + 3 leading data and API aggregators
+
21 apps connected to at least three of the 16 initially selected
=
37 apps and services actively participating in mHealth data sharing
192 data sharing connections (Figure 3)
26 apps and services providing data sharing platforms
21 apps and services providing data sharing platforms with open docs
19 apps and services providing web data sharing platforms with open docs
21 apps and services providing web data sharing platforms with open docs, including 2 manually selected medical apps

**Figure 1. Case Selection**

## 3.2 Research Approach

To understand the design and governance decisions that platform providers make to manage how third parties use their Web data-sharing platforms[6], we analyzed the 21 platforms' boundary resources. Figure 2 presents our research approach that included an inductive content analysis, a commonly used method to classify written or spoken materials into categories (e.g., Cho & Lee, 2014). After we selected the cases, we conducted open coding on the API reference documents. Open coding refers to the process in which one attaches labels to data to develop codes that accurately describe or classify the phenomenon of interest (Flock, 2009). In practice, we labeled any information that could pertain to the research question (i.e., any factors that potentially defined how platform providers manage data sharing). When coding subsequent documents, we mapped information to the previously emerged codes whenever possible or added new codes when necessary. After we initially coded all API references, we revised the codes: we aggregated codes with similar meaning and omitted irrelevant ones. After that, we revisited the data using the revised list of codes and tabulated the resulting factors that affect platform use. The table included the factors (code labels) as columns, APIs as rows, and the values of the factors as cells. We first coded API references and other technical documents and after that API license agreements. We also used other sources, such as developer forums, when needed (e.g., to fill missing information or resolve ambiguities). During the process, we conducted three unstructured interviews with technology experts to check our general research logic and initial findings. After we completed the coding stage, we conducted cross-case comparisons in which we looked for differences in the mHealth data-sharing platforms' boundary resources. Further, we selected only those data-sharing design and governance factors that differed for at least two platform APIs and formalized them as data-sharing design and governance decisions. We followed the logic that, if different data-sharing companies handled an issue in a different way, such companies could choose between several options to handle the issue. Further, by comparing multiple cases, we could gather different options or alternatives for each design and governance decision. We also elaborated on the decisions based on the reviewed documentation and supplementary Web material and categorized them based on their focus. In addition, we conducted two semi-structured research interviews with the API experts from wearable device companies to refine the decisions we identified and understand platform providers' motivation for making particular decisions. We reference the insights that the interviewed experts shared with the codes WD1 and WD2.

[6] Hereafter, we refer to "Web data-sharing platforms" to as "data-sharing platforms" for brevity.

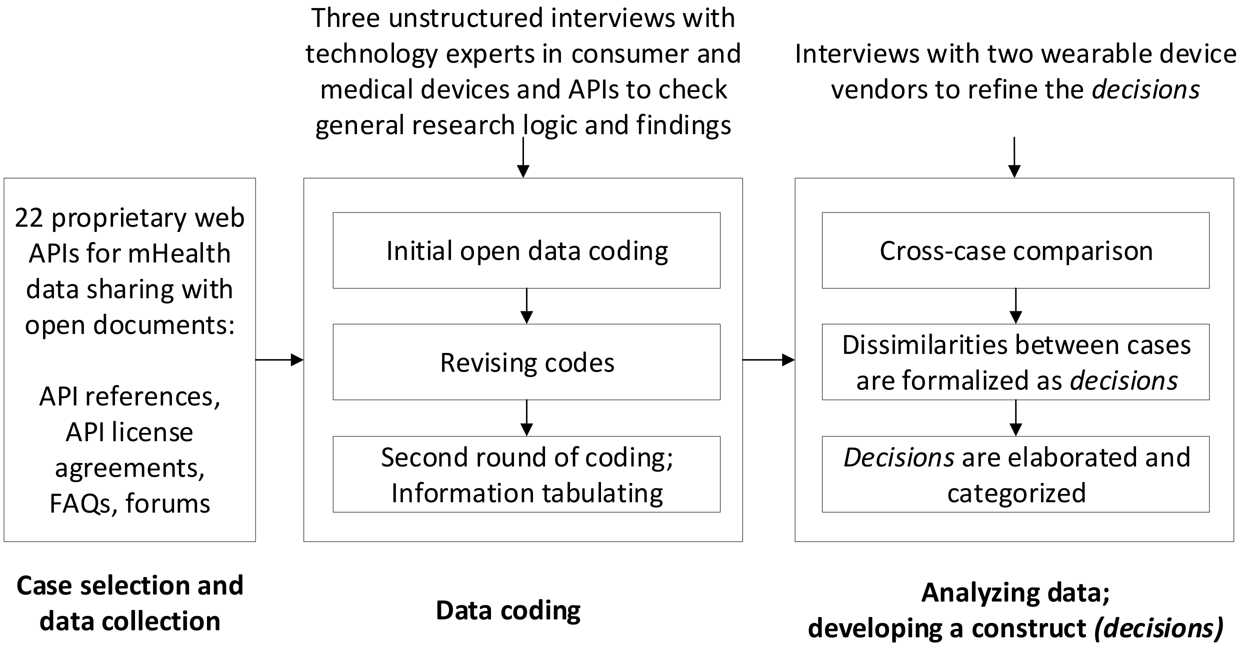
Three unstructured interviews with technology experts in consumer and medical devices and APIs to check general research logic and findings
Interviews with two wearable device vendors to refine the *decisions*
22 proprietary web APIs for mHealth data sharing with open documents:
API references, API license agreements, FAQs, forums
Initial open data coding
Revising codes
Second round of coding; Information tabulating
Cross-case comparison
Dissimilarities between cases are formalized as *decisions*
*Decisions* are elaborated and categorized
Case selection and data collection
Data coding
Analyzing data; developing a construct *(decisions)*

**Figure 2. Research Approach**

# 4 Design and Governance Decisions of Web mHealth Data Sharing

Table 1 presents 18 key design and governance decisions that regulate the Web platform-based mHealth data sharing, alternatives for each decision, and examples that show the choices that two large wearable device producers (Fitbit and Polar) made. We list only the most important decisions rather than them all based on the platform cross-case comparison. We divide the decisions into four groups: 1) high-level data-sharing strategy, 2) data-scope governance, 3) platform design, and 4) platform-governance decisions. While the first group covers decisions that any stakeholder participating in data sharing must make, the second one pertains to data providers and platform providers, and the last two groups pertain to platform providers. At the same time, complementors (platform consumers) can use the table as a tool to evaluate potential data-sharing collaborations with platform providers.

## 4.1 High-level Data-sharing Strategy

First, an mHealth company has to define its data-sharing role (Decision 1); namely, whether it provides, consumes, or both provides and consumes mHealth data (data prosumers). This decision connects to a company's type and services. Thus, data producers typically manufacture devices (e.g., Polar) and/or provide other service that facilitate data logging (e.g., calorie counter MyFitnessPal), whereas data consumers use the data that producers generate to, for example, provide wellness coaching (e.g., Tactio Health). Some data providers can also be prosumers, such as Fitbit (Table 1), which not only allow others to access data from its service but also receive data from other mHealth data providers.

Next, a company must define its data-platform role: platform provider, consumer (also known as complementor), or prosumer (Decision 2). Designing and supporting a platform requires considerable investment, and companies run the risk that they will not be able to attract complementors. Therefore, in the mHealth ecosystem where many companies have a data-sharing platform (which includes the aggregator platforms that Apple, Google, and Samsung operate), organizations can often share data by connecting to desirable collaborators' platforms. On the other hand, by deploying such integrations, companies come to depend on platform providers, which can change their API at any moment and lead to breakdowns in the platform consumer's services (e.g., Rafiq, Ågerfalkm, & Sjöström, 2013) or discontinue the complementors' access to the platform altogether. Therefore, the decision whether to rely on partners' platforms, to open one's own platform, or to combine the two has strategic importance in data sharing. When deciding a data-platform role, mHealth companies must particularly consider the extent to which they will use data aggregator (hub) platforms, such as Google Fit and Apple HealthKit. Data hubs have many benefits: for instance, they can facilitate data sharing by eliminating the need for peer-to-peer integrations (Apple, n.d.). Therefore, some mHealth companies implement a connection to Apple Health or Google Fit as their first (and sometimes only) integration (e.g., Oura Ring and Xiaomi). At the same time, hubs do not seem to completely substitute proprietary platforms. Thus, for example, in October 2017, Polar opened its previously moderated API rather than expanding data sharing through hubs.

**Table 1. Key Design and Governance Decisions for Managing Web mHealth Data Sharing**

| Decision | Alternatives | Ex.1: Fitbit | Ex.2: Polar |
|---|---|---|---|
| **High-level data sharing strategy (all actors)** | | | |
| 1) Data-sharing role | Data provider, consumer, or prosumer | Data prosumer | Data provider |
| 2) Data-platform role | Platform provider, consumer, or prosumer | Platform prosumer | Platform prosumer |
| **Governance of data scope (data providers, platform providers)** | | | |
| 3) Data types shared | Limited or not limited. (Provided: all collected or some. Accepted: custom data types allowed or not) | Provided: not limited (all collected)<br>Accepted: custom data not allowed | Provided: limited (except sleep data) |
| 4) Granularity of provided data | Limited or not limited. (Provided: summaries/ samples or most granular available. Accepted: granularity restricted or not) | Provided: limited for heart rate and activity data; not limited with special permission<br>Accepted: limited (no time series logging) | Provided: limited (no granular daily activity data) |
| 5) Timeliness of provided data | As soon as available or delayed | As soon as available | As soon as available |
| **Platform design (platform providers)** | | | |
| 6) Number of APIs to a data platform | One or more | One | One |
| 7) Platform API rights | Read, write, or both | Both | Read only |
| 8) Architectural style of API | REST API or other | REST API | REST API |
| 9) Data change detection mechanisms | Polling, pull notifications, subscription API ("webhook") | Subscription API | Pull notifications |
| 10) Data access authorization | OAuth (1 or 2: authorization code grant or other grant type), or other | OAuth 2.0: Authorization code grant, Implicit grant | OAuth 2.0: Authorization code grant |
| 11) Supported data format | JSON, XML, FIT, GPX, TCX, or other | Read: JSON, TCX; Write: JSON | Read: JSON, XML, FIT, GPX, TCX |
| **Platform governance (platform providers)** | | | |
| 12) Platform openness | Open, semi-open, moderated, or hidden | Semi-open, access to granular data requires special permission | Open |
| 13) API usage-rate limits | Yes or no | Yes | Yes |
| 14) Price of API usage | Free, paid, or freemium | Free | Free |
| 15) Revenue sharing / affiliate program | Yes or no | No | No |
| 16) Directory of partners using API | Yes or no | Yes | Yes |
| 17) Secondary sharing of data that platform provides | Prohibited or not explicitly prohibited | Prohibited | Not explicitly prohibited |
| 18) Platform consumers' use of historical data after the integration is terminated | Prohibited or not explicitly prohibited | Not explicitly prohibited | Prohibited |

Figure 3 illustrates the data-platform roles of mHealth companies active in sharing. To identify a company's data-platform role, we examined 192 direct data-sharing links between 37 studied mHealth companies (see Figure 1). We identified the links via searching the Web and conducting app-usage experiments. For each integration, we defined the two parties that participated in data sharing as either a resource provider (API and platform) or a client. We identified the resource provider (API) by spotting which service provider authorizes a connection. To do so, we relied on OAuth: a standard in mHealth that organizations use to enable an end user (resource owner) to grant websites or applications (client) access to the information stored in another website (resource server) without disclosing the password.

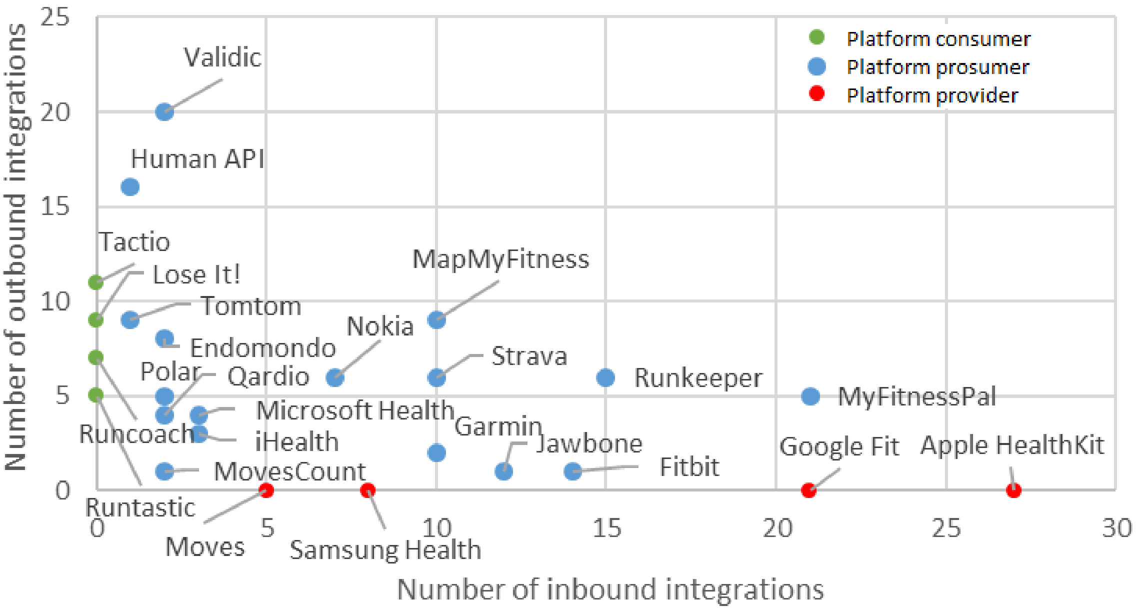

**Figure 3. mHealth Data-sharing Apps and Services by the Number of Inbound and Outbound API Integrations**

Figure 3 indicates the number of inbound and outbound integrations between the 37 mHealth companies we studied. Each point's color indicates a company's data-platform role: red for (clear) platform providers, green for (clear) platform consumers, and blue for platform prosumers. Out of the 37 companies we studied, four represented platform providers, 11 represented platform consumers, and the remaining 22 represented platform prosumers (the figure does not depict them all). Depending on the relation of inbound and outbound integrations, some prosumers represented a platform provider more than consumers. For example, Jawbone and Fitbit had only one outbound integration but more than 10 inbound integrations, which shows that they mostly shared data using their own APIs. On the other hand, Tomtom and Endomondo had considerably less inbound integrations than outbound, which means that they mostly represented platform consumers.

Overall, a company planning to participate in data sharing can define its high-level strategy and position itself by choosing between 15 possible combinations of the four elementary roles that we present in Table 2. These roles build on a company's data-sharing role and data-platform role. The elementary roles A, B, C, and D represent "clear" production or consumption roles that exclude data and platform "prosumption". The prosumption roles exist in multiple configurations, which the four elementary roles in combination describe. For example, Fitbit followed the ABCD configuration (data prosumer/platform prosumer). In turn, Polar followed the AB configuration (data provider/platform prosumer). Finally, Google Fit and Samsung Health followed the AC configuration (data prosumer/platform provider).

**Table 2. High-level Data-sharing Strategies**

| | **Platform provider** | **Platform consumer** |
|---|---|---|
| **Data provider** | A | B |
| **Data consumer** | C | D |

After a company chooses a high-level data-sharing strategy, data providers and platform providers (roles A, B, and C) must decide how they will govern data scope (see Section 4.2), and platform providers (roles A and C) must additionally decide how they will design and govern their platform (see Sections 4.3 and 4.4). Companies must make different although interconnected decisions for each component in their high-level data-sharing strategy. For example, as a data provider/platform provider (role A), Polar would need to decide on the data it shares through its platform and define how it would design and govern its platform. In turn, as a data provider/platform consumer (role B), Polar would need to decide on the data it shares through each third party's platform.

## 4.2 Governance of Data Scope

If a company decides to share data by providing data or a data platform, it further should decide whether to limit the type of data it shares or not (Decision 3). Thus, data consumers/platform providers (role C in Table 2) must decide whether to accept custom data types, although they typically allow only pre-defined data types. Data providers (roles A and B) must decide what available data types they want third-party developers to access. On the one hand, end users own most mHealth data; as such, they should be able to control how other parties use their data. On the other hand, data providers may want to keep some data types private and accessible uniquely from the proprietary service to maintain a competitive advantage (WD1). Thus, for example, Jawbone did not provide "advanced sensor data" such as galvanic skin response and temperature (which many other fitness trackers do not feature) to complementors, and Polar did not provide sleep data to complementors.

Furthermore, data providers can limit the level of detail in the data they provide to others (Decision 4). Thus, many service providers share only summarized data on a daily or per-activity basis (e.g., Tomtom and Misfit). Data providers may use access to granular data as a premium feature. Thus, Garmin delivers a second-level activity data for a US$5,000 license fee, while Fitbit grants access to granular activity and heart rate data only to selected partners. Data consumers/platform providers (role C) can similarly limit data granularity.

Typically, data providers allow consumers to access data as soon as it becomes available on the platform (e.g., Fitbit and Polar). However, in some cases, providers may decide to delay data delivery (Decision 5). Among the data providers we studied, only Dexcom explicitly used delayed data delivery: it sent glucose measurements to partners with a three-hour delay to prevent health-critical data uses (Comstock, 2017). We did not find any such limitation in platforms that enable third parties to write data; therefore, data consumers/platform providers in practice do not seem to make Decision 5.

## 4.3 Platform Design

Service providers that intend to share data through their own proprietary Web platform have to decide whether to provide one or more APIs for the platform (Decision 6). Providing multiple Web APIs implies issuing different API access keys and having a separate developer-registration process. Therefore, multiple APIs may be sensible for separating different groups of platform users as with Validic, which had one API for data providers (typically mHealth companies) and one for data consumers (e.g., healthcare organizations). Furthermore, different APIs may provide access to different data as with Garmin, which had a paid API for granular training data and free API for daily activity data. However, providers typically open one Web API (e.g., Fitbit and Polar).

Service providers that decide to open a web API for data sharing must define whether third parties can use their API to read data from the platform, write it, or for both purposes (Decision 7 in Table 1 and Figure 4). This decision depends on the selected data-sharing role. Thus, for example, if a platform provider represents a data provider (role A), its API should provide "read" rights. All studied APIs (except Validic Connect) allowed complementors to read data. When an API also permits complementors to write data, they can use the platform as a backup or even primary storage location. Twelve out of 22 studied APIs allowed complementors to write data, such as Fitbit, Strava, and Google Fit.

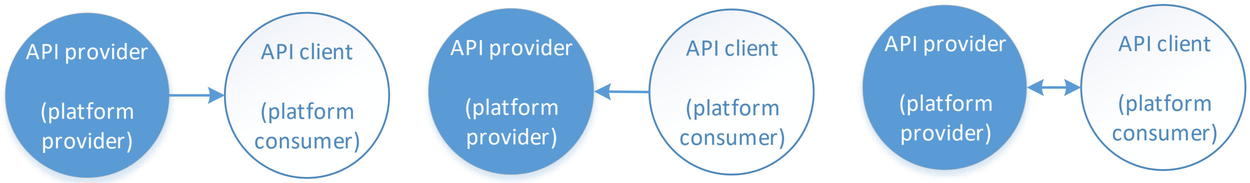

**Figure 4. Possible Web Data-sharing Arrangements (Read Only, Write Only, and Read and Write API Rights); Arrow Shows the Data-flow Direction**

Furthermore, Web platform providers have to choose an architectural API style (Decision 8). Currently, representational state transfer (REST) dominates other Web API architectures due to its simplicity compared to other approaches and its reliance on standard HTTP operations; however, other alternatives exist (Lensmar, 2013). Out of the studied Web API providers, Garmin's Connect API did not seem to comply with the REST architecture because it supported only the "push" data-transfer method (Garmin, n.d.), whereas REST uses the synchronous "pull" data-transfer method in which data consumers can detect changes in data by regularly polling the provider's server. However, apart from standard polling, providers may decide to offer other asynchronous mechanisms for detecting new data (Decision 9), which also deviate from traditional REST architecture. Only platform providers that allow complementors to read data from their platform should make this decision (platform API rights = read or both). Thus, Polar implemented pull notifications in its REST API, which allows data consumers to check whether their end users have any new data available for download. This approach differs from polling in that it requires complementors to send a request to receive information on new data for all authorized users and data types. Fitbit took another approach to notify data consumers: it provided a subscription API (a "webhook") that allowed data consumers to receive a notification that new data has arrived for separate end users. In some cases, access to subscription API requires the provider's approval (e.g., Strava, iHealth).

Service providers can share end users' data if end users authorize such sharing; therefore, planning the data access-authorization mechanism represents a crucial platform design decision (Decision 10). Almost all mHealth APIs we studied used OAuth 2.0, the de facto standard for authorizing Web data sharing. However, some service providers still used the first version of the OAuth protocol (e.g., Nokia, Fatsecret) or client login authentication (PredictBGL). OAuth 2.0 authorization's design requires platform providers to make further decisions, which include defining the scope for what data types the application may access and the method through which end users authorize complementors to access their data on the platform (referred to as authorization grant type). Thus, while Polar used only an authorization code grant type suitable for Web and native apps with a Web-service component, Fitbit also supported an implicit grant type suitable for apps without a Web service.

Finally, API designers should decide the data formats they will support (Decision 11). Most API providers we studied used the JSON format to send and receive data (typical for REST APIs). However, some platform providers additionally supported XML and fitness-specific data formats such as GPX, TCX, and FIT. Thus, in addition to JSON, Fitbit provided training data in TCX format, whereas Polar also supported XML, FIT, GPX, and TCX.

## 4.4 Platform Governance

Platform openness represents perhaps the most essential platform governance decision (Decision 12). Some data-sharing platforms we reviewed (e.g., Polar) adopted an open approach. Open data-sharing platforms allow developers to register, access features, and obtain API keys without restrictions. Semi-open data-sharing platforms provide developers with access to basic features after registration but require the provider's approval to access certain functions (e.g., Fitbit, which kept access to granular data private, and Strava, which enabled a webhook for selected developers). Furthermore, moderated data-sharing platforms grant an API key only when they approve a developer and app. Moderated platforms include MyFitnessPal and Garmin, which did not have openly available documentation for their APIs. Some platforms, such as Dexcom, adopted an open approach for prototyping but a moderated one for the production stage. Finally, one can further classify some moderated platforms as hidden with no public information on their existence. For example, Endomondo has such a platform, which, for example, Tomtom used.

Platform providers can also limit the number of API calls when governing their Web data platforms (Decision 13). For example, providers can set call limits for different periods, such as a minute, an hour, or a day. In the documentation for the 22 APIs we studied, 13 specified call limits, two mentioned call limits but did not specify them, and the rest either did not mention call limits or such limits did not exist.

Furthermore, platform providers must decide whether and how to charge for API access (Decision 14). In mHealth, platform providers typically expect data sharing to pay off indirectly through an increase in their sales and consumer base. Therefore, platform consumers do not typically pay for using the API (e.g., APIs of Fitbit and Polar are free). However, some providers adapted a freemium model in that they charged either for high API usage that exceeded set limits (TomTom, MapMyFitness, Fatsecret) or for access to certain data (PredictBG). Some mHealth APIs adopted a paid model. Thus, Garmin charged a one-time license fee (US$5,000) for access to its Connect API, although it shared less granular data for free through its Garmin Health API. Similarly, Samsung charged for the access to its REST API, although we could not locate any publicly available pricing details. Finally, Validic and Human API provided a commercial mediator service and naturally charged for their service (i.e., API usage). On the other hand, some data providers may decide to share the revenue that data consumer stimulate when using the API (Decision 15). For example, Runkeeper initially gave away 50 percent of the premium service sales driven that its partners drove (Runkeeper, n.d.), although it later shut the referral program down. Thus, revenue sharing does not exist in current mHealth data-sharing platforms.

Web platform providers may further attract more data consumers and increase their sales if they open a partner app directory (Decision 16). Many two-sided markets inherently include such a directory, but not all mHealth data-sharing platforms feature them. Nine out of 21 Web platform providers we studied, which included Fitbit and Polar, had partner app listings on their websites. In some other cases, we could access the information on compatible apps on webpages that explained how to connect the apps (e.g., MapMyFitness) or such information was not available at all (e.g., Nike+ Run).

Due to the high interconnectedness between mHealth companies, data consumer can further send the data that data provider shares to another service provider. Thus, platform providers should decide their position on such secondary sharing of data they provide (Decision 17). Some companies such as Polar did not explicitly prohibit such sharing, whereas Fitbit and Dexcom did not allow it. Some end users exploit secondary sharing to enable a data flow between indirectly integrated services (Long, 2015).

Finally, platform providers must decide whether platform and data consumers can use data shared with them after the integration between platform provider and consumer ends (Decision 18). In this situation, some providers (e.g., Polar) required consumers to delete all data they received, which may constitute a switching cost for data consumers given the potential importance of historical data for improving algorithms and services (due to the so-called “data network effect”) (Turck, 2016). At the same time, platform providers may not easily be able to monitor whether data consumers fulfill this condition. Some other platform providers, such as Fitbit, had license agreements that did not explicitly prohibit data consumers from using historical data after an integration’s termination.

# 5 Discussion

## 5.1 Impact of Design and Governance Decisions on Generativity and Control

Table 1 defines decisions that companies must make to manage mHealth data sharing and resolve the tradeoff between enhancing generativity and maintaining control. Thus, without proper control, an mHealth company that wants to increase the value of its own mHealth service by allowing others to access its data and enabling new use cases may lose a competitive advantage. While the first two decisions in Table 1 determine a company’s roles and high-level data-sharing strategy, the other 16 decisions can have a greater or lesser effect on platform generativity or control. Thus, by regulating the scope of the data that they make available (Decisions 3-5), data providers can affect their generativity by changing shared data’s adaptability[7] as Figure 5 shows. Indeed, fewer data types, lower data granularity, and delayed data delivery result in less adaptable data and restrict the innovative applications and services it can enable. At the same time, providing limited data does not challenge the provider’s competitive position.

[7] Hereafter, we refer to the generativity factors as according to Zittrain (2008) as we describe in Section 2.2

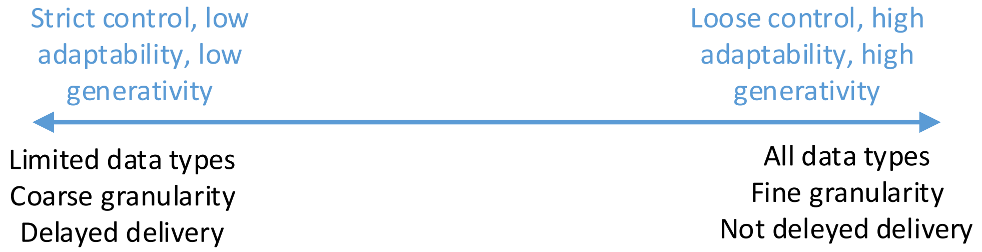

**Figure 5. Relationship between Shared Data, Control, Adaptability, and Generativity**

Platform providers may also use other decisions (Decisions 6-18) to manage their data platform and data sharing. Some decisions directly relate to platform generativity and control, some indirectly relate to it, and, in some cases, an increase in platform generativity does not come at the cost of less platform control. For example, openness (Decision 12) immediately affects a platform's control and generativity through accessibility. Similarly, API usage-rate limits (Decision 13) can restrict a platform's accessibility and adaptability while allowing stricter control. In practice, platform providers impose API usage-rate limits to protect their servers against negative impact on service quality due to too many requests (WD2) or use it as a differentiator between free and premium services. Charging for API usage (Decision 14) can decrease platform accessibility and, therefore, generativity, while sharing the revenue (Decision 15) will likely have the opposite effect. Further, having a partner directory (Decision 16) can increase platform leverage and, therefore, motivate some third-party developers to join the platform. Similarly, non-prohibitive policies on secondary data sharing (Decision 17) and data use after a data-sharing integration's termination (Decision 18) may have a positive effect on platform generativity (adaptability and accessibility).

Platform design decisions typically have a less evident impact on generativity or control than platform governance- and data scope-related decisions do. Thus, platform providers can use several APIs (Decision 6) to separate platform consumers into different groups (e.g., data providers and data consumers) and tune platform openness and control with greater granularity. Although having several platform APIs instead of one may decrease platform accessibility for some platform consumers, for others, providing several APIs with clearer focus may enhance the ease with which platform consumers can master the platform. Further, expanding platform API rights (Decision 7) from read only to read and write can open new platform uses and, hence, potentially increase platform leverage. Finally, a platform's technical functionality (Decisions 8-11) can indirectly affect platform generativity through ease of mastery: the more familiar to third-party developers the platform functionality, the lower the learning curve, and the easier users can use the platform.

## 5.2 Challenges of mHealth Data Sharing Design and Governance

Apart from managing the tradeoff between promoting generativity and keeping control, in managing mHealth data sharing, platform providers face other challenges that the industry as a whole needs to address to increase the benefits from sharing data. Table 3 summarizes eight such challenges that we identified based on analyzing boundary resources and research interviews.

We found that data consumer and provider roles typically operate separately from each other, which means that data prosumers do not commonly appear in mHealth even though many data providers can benefit from using complementary data that other parties generate—likely because some providers have concerns about using other companies' data due to its unknown quality (WD2). Uncertain data quality constitutes a central problem in the data economy (Challenge 1), which calls for organizations to establish quality-control mechanisms (Koutroumpis, Leiponen, & Thomas, 2017).

Furthermore, with multiple data-sharing platforms, some platform providers could remain unconnected due to their mutual unwillingness to make yet another investment in establishing and maintaining an integration to another company's platform (Challenge 2). Recently emerged data aggregators or hubs, such as Google Fit and Apple Health, improve the interconnection in the industry and data-sharing efficiency by decreasing the number of required integrations. However, hubs do not seem to completely substitute for proprietary platforms partially because they use data models that do not suit some mHealth companies (WD1) (Challenge 3). Furthermore, the unwillingness to collaborate with hubs may also relate to the potentially negative business impact from such collaboration (Challenge 4). Namely, sharing data through a hub implies that a company loses control over the process as the data uploaded to such platform becomes available to other platform participants under the license terms that the platform provider defines. This loss of control may explain why some service providers, notably Fitbit, did not share any data with hub platforms. Therefore, hub platform providers should increase the attractiveness of their platforms to data providers by, for example, enhancing the potential value that data-providing complementors gain from consuming data (e.g., through promoting the diversity of available data types and assuring data quality).

While data overprotectiveness inhibits data sharing, some mHealth companies, particularly wearable device producers, willingly outsource a service part of their product to complementors and, therefore, make all data that their devices capture available to others (WD1, WD2). Such companies seem to view themselves predominantly as hardware business and do not pay as much attention to providing services as they do to producing devices. Although this approach works well for device producers now, it may pose a challenge in the future with the commoditization of sensors (Challenge 5). Similar to handset industry, mHealth can move from the hardware to software and service-driven stage of development (Kekolahti, Kilkki, Hämmäinen, & Riikonen, 2016) once the hardware starts to be good enough for the average consumer's needs. In fact, the commoditization of wearable devices has already seemingly begun. Xiaomi, a Chinese manufacturer that offers low-priced fitness trackers, was the second largest wearable device producer by units shipped in 2017 (IDC, 2018). Despite the low price, researchers found Xiaomi Mi 2 Band to be as accurate as the nearly three times more expensive Fitbit Charge HR (Tam & Cheung, 2018). As such, we can see that differentiating hardware has become more difficult and that competition may gradually shift from focusing on devices to services and the third-party developer ecosystem. Therefore, device producers should focus more on providing in-house services and pay higher attention to how they govern data sharing.

The debatable sustainability of free data sharing that currently prevails in mHealth may pose another challenge (Challenge 6). Indeed, organizations commonly share mHealth data without charge since collaborations add value to both data providers' and data consumers' services, while the party that will likely benefit more typically pays for deploying the integration. However, maintaining the platform costs money as well, and some platform providers seem to find it difficult to monetize data sharing indirectly through additional sales, which may explain why some providers, such as Runkeeper, stopped accepting new developer registrations (WD1) and why other platform providers stopped updating their API. One potential way to resolve this problem involves applying an Internet peer-like pricing: if both parties equally benefit from the connection, then the platform consumer does pay a fee for API access. However, if one party will benefit more, it may have to pay not only for the deployment of the integration but also for the API access. This solution, however, will increase the transaction cost of establishing data-sharing collaborations. Nevertheless, with the commoditization of wearable devices and growing competition on mHealth's hardware side, charging for API access in the future may be a reasonable revenue opportunity for device producers.

Furthermore, sharing data in mHealth involves challenges that relate to the need to comply with numerous regulatory requirements (Challenge 7). For example, in the European Union, the General Data Protection Regulation (GDPR) regulation protects mHealth data. The regulation defines (among other things) requirements and lawful basis for personal data processing (Eur-Lex, 2016). Some interpretations understand mHealth data as sensitive personal data (Malgieri & Comandé, 2017) that organizations can process based on special lawful grounds, such as receiving explicit user consent, which users typically provide when installing an application. Enabling data sharing requires an organization to obtain a separate explicit authorization that they generally implement with the OAuth 2.0 standard (see Section 4.3). After a data provider transmits data to a complementor, the receiving party's terms govern it, which puts additional pressure on data providers and potentially motivates them to choose a moderated rather than an open data-sharing mode (see Decision 12, Table 1). Overall, although the highly interconnected mHealth industry poses significant privacy and security concerns related to the unauthorized secondary use of data, the GDPR should force service providers to pay higher attention to this issue.

In addition to regulations, a company involved in sharing mHealth data should consider potential ethical concerns (Challenge 8). Thus, an important ethical challenge arises when sharing mHealth data with an insurer in exchange for discounts. While such sharing should have positive implications by promoting a healthy lifestyle and enabling savings, it may also lead to discrimination against people that fail to hit the activity goals that the insurer sets. As such, data-sharing companies need to clearly describe to end users how data consumers will use the data that end users authorize for sharing and what consequences they could face from sharing their data.

Table 3. Summary of Identified Challenges of mHealth Data Sharing

| Challenge | Potential solution |
|---|---|
| 1) Hesitance to use the data due to its unknown quality | Introduce data quality-control mechanisms |
| 2) Hesitance to connect to a platform due to high integration costs | Harmonize APIs along the industry to reduce the cost of integration; share the integration cost; use hub platforms to exchange the data |
| 3) Platform providers provide data models that do not suit complementors' needs | Develop a standardized industry-wide data model |
| 4) Data providers' unwillingness to upload data to platforms (particularly hubs) due to the loss of data-sharing control | Motivate data sharing by, for example, promoting data consumption and data complementarities. |
| 5) The commoditization of hardware may weaken hardware producers' competitive position | Increased focus on providing services and governing shared data |
| 6) Potentially unsustainable free data sharing | Apply Internet peer-like pricing for shared data |
| 7) Regulatory requirements | Use authorization mechanisms to obtain end-users' consent for data sharing; screen complementors based on their data use and protection policies |
| 8) Ethical concerns | Demand complementors to describe how they will use shared data and what consequences users will face from sharing their data |

# 6 Conclusion

In this paper, we analyze the boundary resources of 21 web mHealth data-sharing platforms and identify 18 key design and governance decisions that platform providers must make to manage data sharing in mHealth. In order to select platforms to analyze, we investigated 192 data-sharing integrations between 37 mHealth companies that most actively participated in data sharing at the time we conducted the study. In doing so, we could uncover the mHealth data-sharing landscape (see Figure 3) and define high-level data-sharing strategies. Furthermore, we discuss the impact that the identified decisions may have on generativity, control, and related competitive risks. Finally, we determine challenges in designing and governing mHealth data sharing.

We found two decisions to determine a company's high-level data-sharing strategy: its data-sharing role and data-platform role. In making these decisions, a company can choose to become a provider, consumer, or both in combination (a prosumer). We discovered that, due to multiple possible configurations of data and platform prosumption, companies can choose between 15 high-level data-sharing strategies, which we define as combinations formed from four elementary "clear" data and platform roles (see Table 2). We found that mHealth data sharing commonly includes the platform prosumer role, which means companies often not only provide a platform to third parties but also connect to other mHealth companies' platforms. As such, the mHealth data-sharing ecosystem differs from some other platform ecosystems where platform providers and consumers (complementors) have clearly separated roles. We further discovered that not only platform providers (roles A and C in Table 2) but also data providers (role B) can manage data sharing, which can often regulate the scope of opened data even if they use another party's platform to share data. However, apart from decisions related to governing data scope (Decisions 3-5 in Table 1), platform providers may use other decisions that platform consumers cannot use as levers for managing data sharing (Decisions 6-18). Moreover, the platform provider has the ultimate power to discontinue a complementor's platform access, although such incidents can decrease the platform's attractiveness to complementors.

This paper makes several contributions to theory and practice. First, the results can help managers make decisions about designing and governing data sharing, particularly in mHealth. Thus, an mHealth company can first define its high-level data-sharing strategy using Decisions 1-2 and Table 2. Further, prospective platform providers (roles A and C in Table 2) can consider the identified decisions (namely, Decisions 3-18) and their potential impact (Section 5.1) when designing and governing their platform. In turn, platform consumers (roles B and D) can use our findings to evaluate potential collaborators (i.e., platform providers). Moreover, our discussion on the challenges in designing and governing mHealth data-sharing can benefit industry by drawing attention to the issues that companies should address to improve data sharing’s value. Although in this paper we focus on mHealth, which features unique characteristics (e.g., multiple small data providers connected P2P, sensitive shared data), our results may pertain to other domains where sensitive user data is shared and data sharing can similarly challenge the provider’s competitive position. For example, our results may prove useful to other consumers in IoT domains, such as smart homes or smart cars, where Web data-sharing platforms have started to emerge (Coppola & Morisio, 2016). Further, we contribute to more general literature on platform design and governance by analyzing increasingly ubiquitous data-sharing platforms and identifying unique design and governance decisions inherent to this platform type. Further still, we analyze access API-based platforms, which appear to use certain design and governance mechanisms specific to this platform’s architecture type, such as API usage-rate limitations. Finally, we contribute to the literature on data sharing, which has previously mostly focused on data sharing in the public domain or bilateral agreement-based data sharing between trusted partners.

As with any other study, ours has some limitations that researchers should consider and address in future work. Thus, we mostly considered mHealth apps and services that shared fitness and wellness rather than medical data. We selected such apps and services due to our case-selection procedure in which we picked only companies that actively participated in mHealth data sharing. The rarity of medical data sharing may relate to stricter regulatory requirements imposed on medical mHealth products in general and data sharing in particular. However, future research should pay closer attention to the differences in designing and governing medical and fitness data sharing. Furthermore, although we studied boundary resources in detail, we did not develop apps for the considered platforms, which means that we may not have identified some implicit platform providers’ rules managing the platform and data use. Finally, although we define decisions that mHealth data-sharing companies must make, due to the study’s explorative and descriptive nature, we do not elaborate on the effect that selecting one or another alternative has on platform success. Future explanative studies may build on our results and address this research direction.

## Acknowledgments

The Digital Disruption of Industry (DDI) project, which the Strategic Research Council of the Academy of Finland funds, supported this work. We thank the interviewed experts for the valuable input to this work and Dr. Kimmo Karhu for valuable comments.

## References

Allen, C., Des Jardins, T. R., Heider, A., Lyman, K. A., McWilliams, L., Rein, A. L., Schachter, A. A., Singh, R., Sorondo, B., Topper, J., & Turske, S. A. (2014). Data governance and data sharing agreements for community-wide health information exchange: Lessons from the beacon communities. *eGEMs*, *2*(1), 1-10.

Andreessen, M. (2007). The three kinds of platforms you meet on the Internet. Retrieved from https://web.archive.org/web/20071002031605/http://blog.pmarca.com/2007/09/the-three-kinds.html

Apple. (n.d.). *HealthKit.* Retrieved from https://developer.apple.com/documentation/healthkit

Attard, J., Orlandi, F., Scerri, S., & Auer, S. (2015). A systematic review of open government data initiatives. *Government Information Quarterly*, *32*(4), 399-418.

Bodle, R. (2011). Regimes of sharing. *Information, Communication & Society*, *14*(3), 320-337.

Bucher, T. (2013). Objects of intense feeling: The case of the Twitter API : Computational culture. *Computational Culture.* Retrieved from http://computationalculture.net/objects-of-intense-feeling-the-case-of-the-twitter-api/

Cho, J. Y., & Lee, E.-H. (2014). Reducing confusion about grounded theory and qualitative content analysis: Similarities and differences. *The Qualitative Report*, *19*(32), 1-20.

Comstock, J. (2017). New Dexcom API lets third-party apps access users' glucose data. Retrieved from http://www.mobihealthnews.com/content/new-dexcom-api-lets-third-party-apps-access-users-glucose-data

Constantinides, P., Henfridsson, O., & Parker, G. G. (2018). Introduction—platforms and infrastructures in the digital age. *Information Systems Research*, *29*(2), 381-400.

Coppola, R., & Morisio, M. (2016). Connected car: Technologies, issues, future trends. *ACM Computing Surveys*, *49*(3), 1-36.

de Arriba-Pérez, F., Caeiro-Rodríguez, M., & Santos-Gago, J. (2016). Collection and processing of data from wrist wearable devices in heterogeneous and multiple-user scenarios. *Sensors*, *16*(9), 1538.

Eaton, B., Elaluf-Calderwood, S., Sørensen, C., & Yoo, Y. (2011). *Dynamic structures of control and generativity in digital ecosystem service innovation: The cases of the Apple and Google mobile app stores.* London, UK: London School of Economics and Political Science.

Eaton, B., Elaluf-Calderwood, S., Sørensen, C., & Yoo, Y. (2015). Distributed tuning of boundary resources: The case of Apple's iOS service system. *MIS Quarterly*, *39*(1), 217–243.

Eckartz, S. M., Hofman, W. J., & Van Veenstra, A. F. (2014). A decision model for data sharing. In M. Janssen, H. J. Scholl, M. A. Wimmer, & F. Bannister (Eds*.), 13th IFIP WG 8.5 International Conference on Electronic Government* (pp. 253-264). Berlin: Springer.

Eisenmann, T., Parker, G., & Van Alstyne, M. W. (2006). Strategies for two-sided markets. *Harvard Business Review*, *84*(10), 92-101.

Flock, U. (2009). *An introduction to qualitative research* (4th ed.). Thousand Oaks, CA: Sage.

Förderer, J., Kude, T., Schütz, S., & Heinzl, A. (2014). Control versus generativity: A complex adaptive systems perspective on platforms. In *Proceedings of the International Conference on Information Systems.*

Garmin. (n.d.). *Garmin health API*. Retrieved from https://developer.garmin.com/garmin-connect-api/help/

Ghazawneh, A. (2012). *Towards a boundary resources theory of software platforms.* Jönköping International Business School, Jönköping University. Retrieved from https://www.diva-portal.org/smash/get/diva2:567769/FULLTEXT01.pdf

Ghazawneh, A., & Henfridsson, O. (2013). Balancing platform control and external contribution in third-party development: The boundary resources model. *Information Systems Journal*, *23*(2), 173-192.

Grundy, Q., Held, F. P., & Bero, L. A. (2017). Tracing the potential flow of consumer data: A network analysis of prominent health and fitness apps. *Journal of Medical Internet Research*, *19*(6), e233.

Hagiu, A., & Wright, J. (2015). Multi-sided platforms. *International Journal of Industrial Organization*, *43*, 162-174.

Hein, A., Schreieck, M., Wiesche, M., & Krcmar, H. (2016). Multiple-case analysis on governance mechanisms of multi-sided platforms. In *Proceedings of the Multikonferenz Wirtschaftsinformatik* (pp. 1613-1624).

Helmond, A. (2015). The platformization of the Web: making Web data platform ready. *Social Media + Society*, *1*(2).

IDC. (2018). *Global wearables market grows 7.7% in 4Q17 and 10.3% in 2017 as Apple seizes the leader position, says IDC.* Retrieved March from https://www.idc.com/getdoc.jsp?containerId=prUS43598218

Janssen, M., Charalabidis, Y., & Zuiderwijk, A. (2012). Benefits, adoption barriers and myths of open data and open government. *Information Systems Management*, *29*(4), 258-268.

Kekolahti, P., Kilkki, K., Hämmäinen, H., & Riikonen, A. (2016). Features as predictors of phone popularity: An analysis of trends and structural breaks. *Telematics and Informatics*, *333*(4), 973-989.

Koutroumpis, P., Leiponen, A., & Thomas, L. D. W. (2017). *The (unfulfilled) potential of data marketplaces* (ETLA working papers 53). The Research Institute of the Finnish Economy.

Lee, H. L., & Whang, S. (2000). Information sharing in a supply chain. *International Journal of Manufacturing Technology and Management*, *1*(1), 79-93.

Lensmar, O. (2013). Is REST losing its flair—REST API alternatives. *ProgrammableWeb*. Retrieved from https://www.programmableweb.com/news/rest-losing-its-flair-rest-api-alternatives/analysis/2013/12/19

Long, R. (2015). Stationary waves: Garmin Connect and Google Fit. *Stationary Waves*. Retrieved from http://www.stationarywaves.com/2015/01/garmin-connect-and-google-fit.html

Malgieri, G., & Comandé, G. (2017). Sensitive-by-distance: Quasi-health data in the algorithmic era. *Information & Communications Technology Law*, *26*(3), 229-249.

Manner, J., Nienaber, D., Schermann, M., & Krcmar, H. (2013). Six principles for governing mobile platforms. In *Proceedings of Wirtschaftsinformatik*.

Mello, M. M., Adler-Milstein, J., Ding, K. L., & Savage, L. (2018). Legal barriers to the growth of health information exchange—boulders or pebbles? *The Milbank Quarterly*, *96*(1), 110-143.

Mineraud, J., Mazhelis, O., Su, X., & Tarkoma, S. (2016). A gap analysis of Internet-of-things platforms. *Computer Communications*, *89*, 5-16.

Olla, P., & Shimskey, C. (2015). mHealth taxonomy: A literature survey of mobile health applications. *Health and Technology*, *4*(4), 299-308.

Patel, V. (2015). How to platformize your product: A guide to building APIs. *Developer.com.* Retrieved from https://www.developer.com/design/how-to-platformize-your-product-a-guide-to-building-apis.html

Puschmann, C., & Burgess, J. (2014). The politics of Twitter data. In K. Weller, A. Bruns, J. Burgess, & M. Mahrt (Eds.), *Twitter and society* (pp. 43–54). New York, NY: Peter Lang.

Rafiq, A., Ågerfalkm, P. J., & Sjöström, J. (2013). Boundary resources dependency in third-party development from the developer's perspective. In *Proceedings of the 8th International Conference on Design Science Research in Information Systems* (pp. 197-211).

Research2guidance. (2016). *mHealth app developer economics 2016—the current status and trends of the mHealth app market.* Retrieved from https://research2guidance.com/product/mhealth-app-developer-economics-2016/

Research2guidance. (2017). *mHealth app economics 2017—current status and future trends in mobile health.* Retrieved from https://research2guidance.com/wp-content/uploads/2017/10/1-mHealth-Status-And-Trends-Reports.pdf

Runkeeper. (n.d.). *Introducing the HealthGraph.* Retrieved from https://web.archive.org/web/20160618092527/https://runkeeper.com/developer/healthgraph/introducing-the-health-graph

Schreieck, M., Wiesche, M., & Krcmar, H. (2016). Design and governance of platform ecosystems—key concepts and issues for future research. In *Proceedings of the 24th European Conference on Information Systems.*

Spencer, T., Krohn, A., Fisher, R., & Boyd, M. (2014). API Platform defined: When an API provider is a platform. *Nordic APIs*. Retrieved from https://nordicapis.com/api-platform-defined-api-provider-is-a-platform/

Tam, K. M., & Cheung, S. Y. (2018). Validation of electronic activity monitor devices during treadmill walking. *Telemedicine and E-Health*, *24*(10), 782-789.

Eur-Lex. (2016). *Document 32016R0679.* Retrieved from http://eur-lex.europa.eu/eli/reg/2016/679/oj

Tilson, D., Sorensen, C., & Lyytinen, K. (2013). Platform complexity: Lessons from the music industry. In *Proceedings of the 46th Hawaii International Conference on System Sciences* (pp. 4625-4634).

Tiwana, A. (2013). *Platform ecosystems: Aligning architecture, governance, and strategy*. San Francisco, CA: Morgan Kaufmann.

Tiwana, A., Konsynski, B., & Bush, A. A. (2010). Platform evolution: Coevolution of platform architecture, governance, and environmental dynamics. *Information Systems Research*, *21*(4), 675-687.

Tura, N., Kutvonen, A., & Ritala, P. (2017). Platform design framework: Conceptualisation and application. *Technology Analysis & Strategic Management*, *30*(8), 881-894.

Turck, M. (2016). The power of data network effects. Retrieved from http://mattturck.com/the-power-of-data-network-effects/

Vest, J. R., & Gamm, L. D. (2010). Health information exchange: persistent challenges and new strategies. *Journal of the American Medical Informatics Association*, *17*(3), 288-294.

Wareham, J., Fox, P. B., & Cano Giner, J. L. (2014). Technology ecosystem governance. *Organization Science*, *25*(4), 1195-1215.

Yoo, Y., Boland, R. J., Lyytinen, K., & Majchrzak, A. (2012). Organizing for innovation in the digitized world. *Organization Science*, *23*(5), 1398-1408.

Yoo, Y., Henfridsson, O., & Lyytinen, K. (2010). The new organizing logic of digital innovation: An agenda for information systems research. *Information Systems Research*, *21*(4), 724-735.

Zittrain, J. (2008). *The future of the Internet and how to stop it.* London, UK: Yale University Press.

# Appendix A: Studied mHealth Companies and APIs

Table A1 shows the list of studied mHealth companies that we studied. We detail how we selected these companies in Section 3.1.

**Table A1. The List of Studied mHealth Services and Data-sharing Platforms**

| mHealth service | Platform provider | Selected for study | Link to developers' portal / API reference |
|---|---|---|---|
| Apple HealthKit | Yes | No, not Web API | |
| Argus | No | no | |
| Dexcom* | Yes | Yes, manually selected | https://developer.dexcom.com/ |
| Endomondo | Yes | No, no open docs | |
| Fatsecret | Yes | Yes | https://platform.fatsecret.com/api/ |
| Fitbit | Yes | Yes | https://dev.fitbit.com/build/reference/web-api/ |
| Garmin | Yes | No, no open docs | |
| Glow | No | No | |
| Google Fit | Yes | Yes | https://developers.google.com/fit/rest/ |
| Human API | Yes | Yes | https://hub.humanapi.co/docs |
| iHealth | Yes | Yes | http://sandbox.ihealthlabs.com/ dev_documentation_openapidoc.htm |
| Jawbone | Yes | Yes | https://jawbone.com/up/developer/ |
| Kiqplan | No | No | |
| Lifesum | No | No | |
| Lose It | No | No | |
| MapMyFitness | Yes | Yes | https://developer.underarmour.com/docs/ |
| Microsoft Health | Yes | Yes | http://developer.microsoftband.com/Content/ docs/MS%20Health%20API%20Getting%20Started.pdf |
| Misfit | Yes | Yes | https://build.misfit.com/docs/cloudapi/get_started |
| Moves | Yes | Yes | https://dev.moves-app.com/docs/ |
| MyFitnessPal | Yes | No, no open docs | |
| Nike+ | Yes | Yes | http://dev.nike.com/activities |
| Nokia Health | Yes | Yes | https://developer.health.nokia.com/api |
| Omron | Yes | No, no open docs | |
| Pact | No | No | |
| Pear | No | No | |
| Polar | Yes | Yes | https://www.polar.com/accesslink-api/ |
| PredictBG* | Yes | Yes, manually selected | https://predictbgl.com/api/api-REST.html |
| Qardio | Yes | No, no open docs | |
| Runcoach | No | No | |
| RunKeeper | Yes | Yes | https://runkeeper.com/developer/healthgraph/app-ideas |
| Runtastic | No | No | |
| Samsung Health | Yes | Yes | https://developer.samsung.com/health/server |
| Strava | Yes | Yes | https://developers.strava.com/docs/reference/ |
| Suunto (MovesCount) | Yes | No, no open docs | |

**Table A1. The List of Studied mHealth Services and Data-sharing Platforms**

| | | | |
|---|---|---|---|
| Tactio | No | No | |
| TomTom | Yes | Yes | https://developer.tomtom.com/tomtom-sports-cloud/tomtom-sports-cloud-documentation |
| Wahoo Fitness | Yes | No, not Web API | |
| Validic | Yes | Yes, 2 APIs | https://docs.validic.com/ |
| Vitadock (Medisana) | Yes | Yes | https://github.com/Medisana/vitadock-api/wiki |
| * Manually selected API providers added to account for medical (rather than pure fitness) apps and services to ensure diversity; not among the 37 most actively participating in mHealth data-sharing services | | | |

## About the Authors

**Alexandr Vesselkov** is a doctoral candidate in Network Economics research group at Department of Communications and Networking, Aalto University, Finland. He received his master's degree in Communications Ecosystem from Aalto University in 2014. His research interests include the impact of Internet of things technologies on the transformation of industries, in particular, healthcare; platform economy, as well as techno-economic analysis of new mobile technologies and services.

**Heikki Hämmäinen** is Professor of Network Economics at Department of Communications and Networking, Aalto University, Finland. He has MSc (1984) and PhD (1991) in Computer Science from Helsinki University of Technology. His main research interests are in techno-economics and regulation of mobile services and networks. Special topics recently include measurement and analysis of mobile usage, value networks of flexible Internet access, and diffusion of Internet protocols in mobile. He is active in several journals and conference duties.

**Juuso Töyli** is Professor of Operations and Supply Chain Management at Turku School of Economics at University of Turku and Adjunct Professor of Network Economics at Aalto University. His research interests include policy issues and the diffusion of mobile technologies and their effects. He is further interested in business games and their development. Within operations and supply chain management, his research is mainly focused on firm and supply chain performance (financial, logistics cost and operations performance) and how these are related to various issues like strategy choices, outsourcing, low-cost sourcing, geographic dispersion and sustainability.