Ethics and Information Technology (2019) 21:181–196
https://doi.org/10.1007/s10676-019-09499-x

ORIGINAL PAPER

Digital health fiduciaries: protecting user privacy when sharing health data

Chirag Arora[1]

Published online: 13 February 2019

Abstract
Wearable self-tracking devices capture multidimensional health data and offer several advantages including new ways of facilitating research. However, they also create a conflict between individual interests of avoiding privacy harms, and collective interests of assembling and using large health data sets for public benefits. While some scholars argue for transparency and accountability mechanisms to resolve this conflict, an average user is not adequately equipped to access and process information relating to the consequences of consenting to further uses of her data. As an alternative, this paper argues for fiduciary relationships, which put deliberative demands on digital health data controllers to keep the interests of their data subjects at the forefront as well as cater to the contextual nature of privacy. These deliberative requirements ensure that users can engage in collective participation and share their health data at a lower risk of privacy harms. This paper also proposes a way to balance the flexible and open-ended nature of fiduciary law with the specific nature and scope of fiduciary duties that digital health data controllers should owe to their data subjects.

Keywords Health data · Digital health · Privacy · Transparency · Fiduciary law · Fiduciary relationships

Introduction

Much has been written about the opportunities of a health revolution offered by the recent proliferation of digital devices, associated apps and network based platforms (Lupton 2015). For example, health data such as heart rate, quantified physical activity, sleep quality, etc. can allow individuals to make healthier diet and exercise choices. However, the potential of digital devices in capturing health data to positively transform the health system goes beyond the individual level. In an aggregated form, with collective participation from various users, this data can offer much more valuable insights at a much larger scale. Examples of such insights include an understanding of effects of various environmental factors on human health, development of new exercise and training regimes, correlations between health symptoms and diseases, correlations between disease risk and physical activity, etc. (Lupton 2015). Further, interpreting the significance of health data (such as that captured in a clinical setting or by a self-tracking device-heart rate, physical activity, etc.), even at the level of the individual, is often contingent upon collective participation, as it requires a statistical comparison of a set of data points (Crawford et al. 2015).

Collective participation, however, faces a conflict introduced by privacy concerns of the individual (Evans 2011). The stakes are particularly high for health data, as inappropriate handling of health information can inflict objective harms on individuals (such as discrimination in employment or insurance or loss of reputation) as well as psychological or subjective harm (Gostin and Hodge 2001; Konnoth 2015). Several surveys and polling data across the developed world have shown that many individuals are concerned about health data breaches as well as misuse of breached data (Gostin and Hodge 2001; Patil et al. 2015). A type of 'exceptionalism', in terms of requirement of a higher level of privacy protection for health data has been recognized in past legislation, and has been reinforced by contemporary phenomena such as increased rate of medical identity theft as well as high monetary worth of health data (Martin et al. 2017; Terry 2012). For users to trust digital platforms and

✉ Chirag Arora
c.arora@tue.nl

[1] Section of Philosophy and Ethics, Department of Industrial Engineering & Innovation Sciences, University of Technology Eindhoven, Het Eeuwsel 57, IPO 1.13 5600 MB, Postbus 513, 5612 AZ Eindhoven, The Netherlands

share their health data, these concerns need to be addressed. A prominent response to these concerns has been advocacy for greater transparency and consent mechanisms, which would allow users a better understanding of and control over how their health data is used (Kaplan 2016).

However, transparency and consent mechanisms, I argue in this paper, are inadequate in protecting against privacy harms, or creating trustworthiness required for users to share health data, on account of the 'costs' of transparency. These 'costs' of transparency can be seen as a function of three different factors: accessibility; time required (to access and understand the information); and complexity of the information. I, therefore, further argue that digital health data controllers[1] should be recognized as fiduciaries, such that they are required to keep the interests of the users at the forefront in making decisions about processing of health data. Besides compensating for the unaffordability of transparency, I argue that fiduciary duties impose deliberative requirements on fiduciaries (health data controllers, in this case) that are necessary to cater to the contextual nature of privacy. These deliberative requirements ensure that users can engage in collective participation and share their health data at a lower risk of privacy harms.

Recently, Balkin and Zittrain have suggested that online service providers should be deemed information fiduciaries (Balkin 2015; Zittrain and Balkin 2016). They have pointed out that such a move would require calibration of duties for different kinds of online service providers as a one-size-fits-all approach is unlikely to succeed (Balkin 2014). Here, I have taken up their suggestion and adapted it for the more specific case of digital health data controllers. I argue that health data controllers should be recognized, by law, as fiduciaries and outline the specific duties, as well as the scope of such duties, that digital health data controllers should have as fiduciaries.

This paper is divided into four main sections. In the section on "Transparency", I argue that transparency does not adequately protect health data subjects against privacy harms, or enable users to trust those they share personal data with. I then introduce the concept of fiduciary relationships and discuss the relevant aspects of fiduciary law, including its underlying characteristics, objectives, principles, and reach. This discussion establishes the background for the next section, where I argue that the relationship between digital health data controllers and users should be recognized as fiduciary for three reasons: (a) the relationships shares key features with traditional fiduciary relationships; (b) it involves circumstances similar to those that have led to establishing fiduciary relationships in the past; and (c) fiduciary law is better suited than contractual or statutory law to protect user privacy and enable trust required for sharing health data with health data controllers. In the same section, I then propose an account of the scope of fiduciary duties that digital health data controllers should owe to their beneficiaries (users sharing health data). Finally, I present some of the gaps of fiduciary law, and highlight issues which, even if my proposal is adopted, would continue to demand our attention in the path to ensuring ethical conduct in processing of our health data.

Transparency

As information sharing becomes more ubiquitous, privacy trade-offs have attracted due attention. In recent years, transparency and control approaches (such as 'notice and consent' regimes) have been touted as one of the important measures to help individuals steer through privacy trade-offs (Acquisti et al. 2013; Kaplan 2016). The argument is made that if individuals are informed about how their data will be handled (for example, what is being collected and to whom it is disclosed), then they will be able to decide their preferences regarding privacy protection and disclosure. The utility of transparency has also been recognized through, and embedded into, legislation across the developed world. In the EU, the incoming General Data Protection Regulation (GDPR) recognizes transparency as one of the central principles with regard to processing of personal data (Recital 58, GDPR n.d.; Spagnuelo and Lenzini 2016). It also states that data controllers should provide easily accessible information to data subjects (Art. 12 GDPR n.d.). Similarly, in the United States, the Health Insurance Portability and Accountability Act (HIPAA), through the 'Privacy Rule', demands notification about the use of health information to the respective individuals, documentation of privacy policies, as well as storing of details regarding access of information (for

[1] Here I use the term 'controller' as defined by the upcoming General Data Protection Regulation (GDPR) in the European Union. According to GDPR, a controller "means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data"; where "personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"; and "processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;" (Art. 4 GDPR—Definitions|General Data Protection Regulation (GDPR) n.d.)

example, who has accessed the information) (Farrell 2012; Spagnuelo and Lenzini 2016).

The success of transparency, in alleviating individual privacy concerns, as well as in promoting sharing of data for beneficial purposes (such as research), however, seems limited. The HIPAA Privacy Rule, for example, has been criticized both for allowing too much access to data (as individual concerns regarding sharing of their data for research were not addressed) as well as for restricting sharing of data for useful research (as consent requirements impeded sharing of data) (Evans 2011).

One of the limitations of transparency, I argue, is its cost. This cost can be seen as a function of accessibility, the time required (to access and understand the information), and complexity of the information.

In the case of digital health information, there are few barriers to accessibility as information (regarding privacy policies and use of data) can be made readily available on the platform. Most digital platforms, by legislation or on a voluntary basis, already do share their privacy policies with the users along with certain control mechanisms (such as the 'notice and consent' forms). However, these privacy policies are still 'costly' to users on account of the time required to read them. Studies have shown that users generally do not read these privacy policies, or do so infrequently (McDonald and Cranor 2008). In their own study, McDonald and Cranor (2008) estimated that the annual opportunity cost, in the US alone, for just reading privacy policies of online websites would be in the order of $781 billion.[2]

The actual costs of transparency may actually be much higher, as privacy policies, for most individuals, are hard to read and understand (Jensen and Potts 2004). While data controllers may fulfil their legal obligations related to transparency by providing 'notice and consent' forms and privacy policies, individuals may still be uncertain about what they are consenting to (Barocas and Nissenbaum 2009). This is largely due to the subjective complexity dimension of transparency.

Candeub (2013) provides the example of Sherlock Holmes as a good illustration of the subjective nature of transparency's complexity (or 'computational', the alternative nomenclature used by the author) dimension. In the movie *The Seven-Per-Cent Solution*, Dr. Watson deceitfully arranges a meeting between Dr. Sigmund Freud (relatively unrenowned in the timeline of the movie) and Sherlock Holmes in Vienna. Dr. Watson hopes that Freud would be able to cure Sherlock off his cocaine addiction. When the two meet, Freud, intending to induce a reflection upon Holmes' addiction, asks him, "Who am I, that your friends should wish us to meet?" [(*The Seven-Per-Cent Solution* 1976) quoted in (Candeub 2013)].

Holmes, defeating the question's intended effect, responds with an exhibition of his deductive skills, "Beyond the fact that you are a brilliant Jewish physician who was born in Hungary and studied for a while in Paris, and that certain radical theories of yours have alienated the respectable medical community so that you have severed your connections with various hospitals and branches of the medical fraternity, beyond this I can deduce little. You're married, with a child of... five. You enjoy Shakespeare and possess a sense of honour." [(*The Seven-Per-Cent Solution* 1976) quoted in (Candeub 2013)].

While these facts about Freud were transparent to Sherlock Holmes through the objects in Freud's study, for most other people the same objects would not have made these facts transparent.

While privacy policies may not require a rare genius of Sherlock's capacity to be understood, they do pose a serious challenge for those not well versed with legal terms, the technical know-how related to data analytics, as well as privacy implications of the terms enlisted. Barocas and Nissenbaum (2009) further the claim, by arguing that (current and future) uses of data, to a degree, may not only be difficult to understand but rather unknowable. This unknowability, they claim, follows from the uncertain chain of events linked to the use of data, such as the emergence of new technologies (for example, new analytical tools or advanced algorithms) and new actors (with unknown intentions).

The limits of transparency are further exposed by research indicating that transparency and control might paradoxically increase disclosure of sensitive information (Acquisti et al. 2013). Consent mechanisms can also exploit (known and still unknown) cognitive biases, such as limited attention span, framing effects, and decision making heuristics, in how people interpret and act on available information (Acquisti et al. 2013; Kahneman and Tversky 1979). For example, Adjerid et al. (2013), in a series of experiments, demonstrate how simple misdirections can alter subject perception of privacy risks, even though the objective risks (and corresponding facts) are not altered.

Eventually, rather than being empowered by transparency, the individual (consenting to share their data) has to take a leap of faith and rely on the assumption that the actors involved in the use of individual's data will be committed to a set of ethical principles, professional commitments, and guiding norms and regulations which protect the individual from privacy harms. When the data being shared is particularly sensitive, such as in the case of health data, the individual is in a rather vulnerable position relative to the data controller, decreasing the incentive to share data, even for

[2] The study conducted by McDonald and Cranor (2008) asked 212 participants to skim through online privacy policies and answer simple comprehension questions. It estimated the value of time as 25% of average hourly salary for leisure and twice wages for time at work in the US.

beneficial purposes such as research that may led to discovery of new preventive or treatment mechanisms for various diseases.

Fiduciary relationships

Sharing of personal or sensitive information for individual or social benefits is not unique to contemporary digital platforms. Individuals also share sensitive information with doctors, accountants and lawyers. In such cases, these professionals are bound by duties which restrict the use of such sensitive information in ways that can be harmful to, or against the interest of, the individual. These duties are established through the notion of 'fiduciary responsibility' assigned to some types of professionals, such as doctors and lawyers, with whom sensitive information is shared (Frankel 2010). In this paper, I argue that digital health data controllers should also be assigned an information fiduciary role, wherein, they are required to keep the interests of data subjects at the forefront, particularly with regards to the protection of privacy. However, before presenting an account of why health data controllers should be given such a role, and what that might entail, I will offer a discussion of fiduciary relationships and fiduciary responsibilities in general. This discussion will highlight key features of fiduciary relationships as well as conditions under which those features are advantageous compared to other legal instruments such as contracts.

The nature of fiduciary relationships

Courts recognize fiduciary relationship of various kinds, including, as already mentioned, doctor-patient, attorney-client, trustee-beneficiary relationships. Yet, there seems to be no consensus on a definition of fiduciary relationships (Frankel 2010). While some claim that a lack of definition makes fiduciary law "elusive'' (Smith 2002), others argue that the lack of definition is incidental, or even a necessary, aspect of fiduciary law's "situation-specificity and flexibility'' (Rotman 2011, p. 941). Courts have therefore, based their judgements on particular facts of a case, recognizing the difficulty of providing a universally applicable definition (Frankel 2010). In one case concerning fiduciary law, for example, the English court of appeals remarked that the court "has always been careful not to fetter this useful jurisdiction by defining the exact limits of its exercise" (Rotman 2011, p. 940–941).

Despite this lack of a common definition, fiduciary relations do have some common elements. These elements include:

1. Fiduciaries offer services (rather than products) that are socially desirable (Frankel 2010).

Fiduciary relationships usually involve an expertise being offered as a service to those who rely on the fiduciary. Typically, without the relationship (between those offering expert service and those availing themselves of it) being established as fiduciary in nature, the services would not be able to produce the desirable social effect (in degree or in kind). For example, a client would not be able to trust their attorney with personal information and attorney's advice, without there being a fiduciary relationship between them (where the attorney has a duty to keep the best interest of the client at the forefront).

2. Fiduciaries are entrusted with a discretionary power over the interests of the beneficiary.

Typically, in a fiduciary relationship, the fiduciary agent acts 'on behalf of' the beneficiary (Licht 2016; Smith 2002). The beneficiary entrusts a 'critical resource' or power to fiduciaries, where the fiduciaries are required to act in the interest of the beneficiary (Frankel 2010; Smith 2002). The critical resource may be tangible, such as property or finances, or intangible, such as personal information (such as health details disclosed to a doctor). The entrustment is to enable or facilitate the fiduciary to deliver their services.

3. Fiduciary law (through assigning fiduciary duties and obligations) counters the asymmetrical power relationship between fiduciaries and beneficiaries and protects the beneficiary against opportunism (Licht 2016).

As mentioned above, fiduciaries are entrusted to act on behalf of the beneficiary, giving them control over the interests of the beneficiary. This power over the beneficiary's interests introduces a power asymmetry between the fiduciary and the beneficiaries and gives rise to a common problem among the fiduciary relations, opportunism (Licht 2016). By requiring the fiduciary to act in the interest of the beneficiary, fiduciary law hinders those with a propensity for being self-interested or opportunistic at the expense of the beneficiary, when entrusted with discretionary power over someone's interests.

Why are fiduciary relationships established?

While the elements described above are common features of fiduciary relationships, they do not fully explain the distinction between fiduciary and non-fiduciary relationships. For example, several non-fiduciary relationships are also based on expert services being offered to clients, where the experts can exploit their authoritative or informational advantage for

their own benefit. Electricians, plumbers, teachers, are all examples of professions that provide such services, which do not have fiduciary status. A plumber, for example, may advise you to install a new faucet, even though you may not need one, simply for their own benefit. A doctor, on the other hand, on account of his fiduciary duties, may not ask you to undergo a surgery that you don't need, just because the doctor will earn more money out of it (Drozd and Dale 2006). Why then do we require that some experts have an obligation to keep the interests of their client at the forefront? In other words, why then are some relationships deemed fiduciary by law while others are not? This section aims to highlight some of the justifications for as well as advantages of fiduciary law over other legal instruments, offered by courts and legal scholars.

Historically, acknowledgement of fiduciary relationships can be categorized in two ways (Miller 2011):

a. Status-based
b. Fact-based

As the name suggests, status-based fiduciary relationships are determined through status. If a relationship falls under a category that has conventionally been recognized as fiduciary, then it is deemed as fiduciary. Examples of conventional fiduciary relationships include doctor-patient, attorney client, and director-companies. The conventional status of these relationships descends from English equity courts during and shortly after the middle ages, which deemed a relationship as fiduciary if it was similar to the relationship between a trustee and *cestui que trust*[3] (Miller 2011). For example, (Worthington 2006) writes:

> [F]iduciary law evolved from Equity's regulation of the relationship between trustees and beneficiaries. Over time these rules were extended, with minor modifications, to cover other situations that seemed analogous. Now it is accepted that relationships between directors and their companies, agents and their principals, solicitors and their clients, and partners and their co-partners are all fiduciary. These are all 'status-based' fiduciary relationships. The status itself inevitably attracts fiduciary impositions

A number of courts have since, however, raised objections to the status-based approach to determination of fiduciary status. Justice Dickson, for example, stated in Guerin[4], "It is the nature of the relationship, not the specific category of actor involved that gives rise to the fiduciary duty" (Miller 2011). Similar arguments have since led to efforts to define fiduciary principles, such that facts, rather than status, can be used to determine fiduciary relationships. Defining these principles also allows for making decisions about relationships that are new (such as between health data controllers and users) or may arise in the future.

While there doesn't seem to be a consensus on what facts or conditions are necessary and sufficient for determination of a fiduciary relationship, a number of such conditions have been offered. Here I discuss some of the most important proposed conditions and their possible limitations:

1. Power-dependency and vulnerability

As discussed earlier, fiduciary relationships involve entrustment of discretionary powers to the fiduciary, which they shall use to the interest of the beneficiary. Justice Wilson argues that certain features, which are common among fiduciary relationships, should be used as criteria to determine other fiduciary relationships (Miller 2011). These common features, which can be used as identifying characteristics of fiduciary relationships, according to Justice Wilson, include: (a) a scope for exercise of unilateral discretionary power by the fiduciary over beneficiary's interest; and (b) vulnerability of the beneficiary to the fiduciary holding the discretionary power.

These criteria have, however, met with some criticism, both within and outside courts, as being insufficient reasons for establishing a relationship as fiduciary. Justice Cromwell, for example, argued that not all power-dependency relationships have been and can be deemed fiduciary in nature (Miller 2011). (Biological) parents, for example, are not deemed as fiduciaries, even though children are dependent upon them (Brinig 2011). Similarly, vulnerability, as an indicium for fiduciary relationships, seems too broad and imprecise.

2. Enabling trust in relationships

Beneficiaries place significant trust in fiduciaries by giving away access and control over their resources. By demanding fiduciaries to act against self-interest, and in the interest of the beneficiaries, fiduciary law plays an important role in enabling the beneficiary to trust agents with discretionary power over them.

However, the idea that trust, or need for trust, can be sufficient in itself for establishing fiduciary relationships is also not without its problems. First, contract law can also enable trust between parties by establishing the rules within which the parties must act. Rotman (2011) states that fiduciary law protects not just any relationships requiring trust, but only

[3] Archaic term in English law for beneficiary under a trust (Cestui que trust 2006).

[4] (*Guerin v. The Queen* 1984) was a landmark case regarding Aboriginal rights in Canada, where the Supreme Court stated that the government had a fiduciary duty towards the First Nations of Canada.

those that require *high* trust and confidence. This distinction between the need for trust and high trust seems in need of further elaboration and support. Second, as courts have recognized in some cases, trust may also be *misplaced*, where individuals should not have had expectations of behavior in their interest (Brennan-Marquez 2015). Therefore, using trust as a criterion for establishing fiduciary relationships would require an explanation of why trust is warranted for that specific relationship between a fiduciary and beneficiary.

3. To support equity, as anti-opportunism

The origins of modern fiduciary law, as discussed earlier, can be traced at least as far back as the English equity courts of the fourteenth century (Miller 2011; Smith 2013). The function of equity courts was to hear pleas where the law seemed limited in its invocation of justice, on account of being too general, or where it seemed unable to cater to the specific circumstances of a particular case (Smith 2013). These courts drew from the principles of equity as defined by Plato and Aristotle, which were meant to plug gaps in laws (Rotman 2011; Smith 2013). These gaps in laws existed, according to Plato, because laws aimed for being certain and universal, while human condition tends to lack universality and certainty (Rotman 2011). Many of the hearings in the English equity courts were for charges against "feoffees", who were persons holding legal title on behalf of others in a quasi-trust agreement (Smith 2013). The courts, through several hearings, held that feoffees should not be opportunistic and "faithless'', in taking the entrusted property to themselves (Smith 2013). Smith (2013) and Frankel (2010) provide accounts of how modern fiduciary law originates out of these early litigations against opportunism, and to enable trust between parties.

However, the idea of fiduciary law as a tool against opportunism warrants more examination for a number of reasons. First, if opportunism is "self-interest seeking with guile" as defined by (Williamson 1975), then examples of opportunistic behavior seem much more frequent than the number of cases where fiduciary law is applied. A number of non-fiduciary economic actors, for example, seek self-interest with some guile, without requiring the courts to intervene through fiduciary law. Secondly, as argued before, if an agent is entrusted with power or resources to warrant opportunism, the said agent could also be restricted through contract law. Why then do we require the category of fiduciary relationships? In order to answer that question, we need to examine if fiduciary law has distinct advantages over contract or statutory law in countering opportunism as well as under what conditions those specific advantages can be useful.

Fiduciary Law's advantages over contract or statutory law in countering opportunism Fiduciary law seeks to prevent not just any opportunism, but as Smith (2013) has argued, rather opportunism that is "hard to capture ex-ante" and thus, cannot be countered by general rules. As Smith (2013) notes, this difficulty in capturing opportunism ex-ante is more than a difficulty in description, particularly in cases where an agent has discretionary powers over the others. In such cases of discretionary authority, the agent has a pre-existing informational advantage over the principal. This informational advantage may involve three types of information: *costly, unobservable and unverifiable* (Licht 2016). Information may be costly, for example, when the principal may not be able to monitor the actions of an agent (with discretionary power) as it might be too expensive to do so. With discretionary power, including access, to the principal's resources, an agent may act in ways which may make it difficult for the agent to observe at all, or to observe the circumstances around the actions of the fiduciary to judge whether the agent acted in principal's interest. Finally, even if the principal were to know the circumstances and the actions of the agent, lack of expertise may make it difficult for the principal to judge whether the agent has breached their duties.

While contract law or statutory law (in the form of regulations, for example) can be useful in preventing some types of opportunism, it is not useful in limiting opportunism that cannot be detected (for example, on account of costly, unobservable or unverifiable information). Within economic literature, this problem is often referred to as *incomplete contracting*, referring to the impossibility of anticipation of all future contingencies as well as the infeasibility of codifying instructions to counter all anticipated contingencies (Sitkoff 2011). Further, unlike Williamson's proposed definition of opportunism (as seeking self-interest with guile), opportunism may not always be in the form of a full blown planned deceit. Unexpected circumstances may generate unexpected opportunities for an agent entrusted with power or resources, without them actively seeking such opportunities. In this regard, the use of equity against opportunism requires an open-endedness, which can fill the gaps of prescriptive principles contract laws work on. As I argue later in "Digital health data controllers as fiduciaries" section, dealing with the contextual nature of privacy is one example where fiduciary law can be more advantageous than a prescriptive contractual approach.

Fiduciary law, thus, provides the legal system with a way to counter opportunism which cannot be completely dealt with through contract law. The open-ended approach required to guard against opportunism, that cannot be detected ex-ante, also partially explains the lack of consensus among courts and scholars regarding a common definition for fiduciary relationships and why fiduciary law seems like a "concept in search of a principle" (Miller 2011).

The nature and scope of fiduciary duties

Owing to the open-ended nature of fiduciary law, fiduciary duties are abstract, lacking a consensus on a common definition. Nonetheless, legal scholars and courts generally tend to recognize two fiduciary duties, broadly defined: the duty of loyalty and duty of care (Miller 2011). While there is broad consensus on there being a duty of loyalty (though there may be issues with what exactly that duty entails) (Gold 2013), the duty of care is more controversial.

Miller (2011), recognizing the controversial status of duty of care, defends it as an important fiduciary duty. As the main argument against inclusion of duty of care as a fiduciary duty, he cites it being "indistinguishable in substance from tort duty"[5] (Miller 2011, p. 55). Miller argues that unlike tort duty of care, which prescribes conduct to avoid foreseeable harm, the duty of care within fiduciary law requires *diligence* and *skill*. That is, fiduciaries are not only required to not cause harm to the beneficiary, but they are also required to use their expertise to the best of their knowledge to make sure that the beneficiaries are not harmed.

There is, however, at least one other argument against inclusion of duty of care as a fiduciary duty: the duty of care, particularly, as defined by Miller, seems too expansive and difficult to carry out for a fiduciary. Or, in other words, it makes it too easy for a beneficiary to claim a breach. Smith (2013), for example, argues that the duty of care opens the opposite door for opportunism, the one for the beneficiary. With the requirements of diligence, skill and putting forward one's best efforts, the beneficiaries can claim a breach just for profit, and without any true injury caused to them. Further, as I will explain below, the duty of loyalty can also require the fiduciary to play a more active role in ensuring the interests of the beneficiary are kept at the forefront.

There is broad consensus that the duty of loyalty is central to fiduciary duties, and fiduciary law in general. However, there is some debate on what this duty entails, and particularly to what 'degree' a fiduciary should be loyal to their beneficiary. That is, how far should a fiduciary go in pursuit of beneficiary's interests (and in avoiding fiduciary's own self-interest)? Here, I take the cue from Lyman Johnson's work, where he argues that fiduciary loyalty involves two conditions: minimum and maximum (Johnson 2003). On a similar note and using the discussion presented by Gold (2013), I present two distinct notions of loyalty, which can be taken as minimum and maximum conditions.

1. Loyalty as avoidance of conflict (Minimum condition)—Miller (2011) describes loyalty (or 'faithfulness') as avoidance of conflict. Here, he makes distinctions between two types of conflict avoidance, both of which are deemed necessary fiduciary obligations.

   The first is avoiding conflict of interest, where the fiduciary avoids the conflict between their pursuit of beneficiary's interest and their self-interest. The second type of conflict avoidance is avoiding conflict between the fiduciary's duties to the beneficiary and the fiduciary's pursuit of other people's interests.

   The anti-conflicts rule can be seen as the minimum core of fiduciary duty of loyalty, even though a narrower version of this rule exists (Gold 2013). Under this narrower version, only avoidance of conflict of interest is seen as necessary, while fiduciaries are not required to have undivided attention towards one beneficiary.

2. Loyalty as affirmative devotion (maximum condition)—while the anti-conflict rule only increases chances of the fiduciary ensuring best interests of the beneficiary, loyalty as affirmative devotion requires that a fiduciary does so. A number of court cases, particularly in the United States, have identified fiduciary loyalty as one of affirmative devotion (Gold 2013). In this conception of loyalty, the fiduciary is required to play a more active role in pursuit of beneficiary's interest, producing a similar effect as intended by Miller's conception of diligent and skillful duty of care. As argued before, such a duty can be difficult to enforce, particularly for epistemic reasons, as it is difficult to know and judge whether a fiduciary had an affirmative devotion towards the beneficiary. It can still be a legal duty though, enforceable only in rare circumstances: where the court can deem a breach to have occurred, for example (Gold 2013).

Besides these two conceptions of loyalty, there are a number of other conceptions of loyalty offered by various scholars, who also disagree on what should be the core minimum of fiduciary loyalty (Gold 2013). Some, for example, have argued that affirmative devotion should be seen as the minimum core of fiduciary loyalty. (Gold 2013) provides an account of various conceptions of fiduciary loyalty, demonstrating that no single account is universal enough to be deemed as a minimum core. This, however, does not entail that there is no duty of loyalty, only that such a duty is abstract and depends on the circumstances of a particular relationship. As (Gold 2013) points out, the under-determined nature of the minimum core of fiduciary loyalty does not mean it is an empty vessel. Rather, it points to a pluralism within fiduciary law, which may require reassessment of existing, and more precise formulations of new, specific

[5] Tort law, simply defined, is common law that recognizes legal liability for someone who causes harm to another in the form of a civil wrong (Dobbs 2008).

fiduciary relationships. This pluralism can be embraced and utilized, once the idea of needing a specific conception of fiduciary loyalty can be rejected. An abstract conception of fiduciary loyalty allows for a more dynamic approach to fiduciary duties in specific settings, such that they can be reassessed with time, particularly when there are changes in socio-technical structures. This paper attempts to provide a basis for the need for fiduciary loyalty on part of digital health data controllers as well as specify what such a duty of loyalty should entail.

Digital health data controllers as fiduciaries

Arguments for recognizing digital health data controllers as fiduciaries

In this section, I present three main arguments for recognizing the relationship between digital health data controllers and users sharing their health data as fiduciary: (a) the relationship shares features with traditional fiduciary relationships; (b) the relationship involves circumstances similar to those that have led to establishing fiduciary relationships in the past; and (c) fiduciary law is better suited than contractual law in protecting user privacy and enabling trust required for sharing health data with data controllers.

Before I expand on the arguments for recognizing health data controllers as fiduciaries, however, it is important to discuss what is meant by 'health data'. As discussed before, previous legislations in the developed world have afforded a higher level of privacy protection for health data (Bywater and Armstrong 2015; Terry 2012). Yet, these legislations, such as the EU data protection directive (DPD), which has now been superseded by GDPR, do not define health data (Bywater and Armstrong 2015). Defining health data can be particularly hard in the present context, where 'health' apps collect a variety of data (such as location data) which may or may not reveal the health status of a person. While providing a full discussion on the definition of health data, and its precise formulation, is beyond the scope of this paper, the definition proposed by Article 29 Working Party (2015) is useful. According to this proposal, personal data qualifies as health data when it meets at least one of the following criteria:

1. It is clearly/inherently medical data
2. It is raw sensor data which can be independently, or in combination with other data, used to draw conclusions about health status or health risk of an individual
3. It allows for reasonable conclusions to be drawn about an individual's health risk or health status, irrespective of accuracy, legitimacy or adequacy of these conclusions[6].

One problem with this definition, which the Article 29 working party also notes, is that it may make the definition of health data seem too broad. Given the argument of this paper, one might worry that such a broad definition would impose fiduciary duties on an overly wide range of data controllers (Article 29 Working Party 2015). One important merit of this definition, however, is that it is able to include data controllers who collect data outside traditional healthcare settings. This is crucial as in this digital age a lot of health data, worthy of protection, is collected outside traditional health settings.

In order to reach a balance between not making the definition too broad, while also included data controllers who collect data through, say, mobile apps and wearable devices, I propose that fiduciary duties be imposed on health data controllers who (a) Process data with the intention of using the data to determine the health status of a specific person[7], or (b) Collect raw data in situations where it will be reasonable for a data subject to conclude that the data is being collected to determine their health status. The first criterion is to ensure that raw data which may not seem to be health related in an obvious way, but is then used in a way that the health status of the data subject is revealed, is also protected. Raw data, which may not seem like health data, when collected over long periods of time, or combined with other data, for example, may reveal the health status of specific individuals and needs protection. At the same time, according to this criterion, data controllers who process such raw data, but do not intend to use it to determine the health status of a specific person, would not be charged with fiduciary duties. Yet, there is a risk here that some data controllers may collect sensitive health data, which would be worthy of protection, but claim that they do not intend to use it to determine the health status of specific subjects. This could, for example, be the case with data collected through sensors

[6] While this clause may make the definition of health data employed here seem broad, the working party argues that it actually excludes a category of personal data from being categorized as health data (using the criterion that these conclusions be reasonable and about the specific individual). For example, data about number of steps taken by the data subject in a single walk, without being combined other data about the same data subject, would not divulge health risk or status of the specific data subject and therefore, would not be regarded as personal health data. For a more detailed account of the merits and demerits of this definition, see the annex to (Article 29 Working Party 2015).

[7] Article 29 working party also proposes a similar criteria but does not include it in their definition of health data (Article 29 Working Party 2015).

on mobile or wearable devices, where the data subjects may reasonably conclude that the data is collected for health related purposes (because, for example, the marketing of the device may suggest that data is being collected in the interest of individual or public health). The second criterion I have proposed plugs this loophole.

With this working definition, I argue that digital health data controllers share features of traditional fiduciaries in that they offer socially desirable services and enjoy a significant advantage over the users from whom they collect health data. There is an asymmetrical relationship between the users and the digital health data controllers, as users typically lack expertise, information about digital health data controllers as well as information about the actions digital health data controllers might take with the user data. This vulnerability of the users relative to the digital health data controllers can be seen as grounds for establishing a fiduciary relationship, as has been argued by some scholars and courts.

As discussed earlier, fiduciary relationships are also established on grounds of enabling trust. Digital health data controllers, in some cases, also put themselves forward as trustworthy organizations that will not misuse user data and present themselves as acting in the interest of their users (for example, Fitbit Privacy Policy 2016). At the same time, digital health data controllers do not disclose full details about their handling of our data [and sometimes for good reasons such as security (as disclosing detailed data security measures can be jeopardizing) and competitiveness]. This incomplete disclosure, coupled with the high costs of transparency, can create a lack of trust among the users, eventually leading to non-participation (by not sharing data, for example) in the promised digital health revolution. Fiduciary relationships between the users and digital health data controllers, where the latter is required to act in the interests of the users, can therefore, be valuable in making data controllers trustworthy and facilitating collective participation.

The need for establishing trust and compensating for vulnerability, however, as argued earlier, may not be sufficient for establishing fiduciary relationships, even though they may have advantages. The third and most important reason for establishing fiduciary relationships between data subjects and data controllers with whom health data is shared, I argue, is that fiduciary relationships are better suited than contractual or statutory obligations [such as those associated with privacy agreements users click 'agree' on their digital devices (contractual) or defined through legislation (statutory)], for protection of user privacy or for balancing protection of privacy with other goals related to societal interests.

To this end, I argue that stringent privacy protection is difficult to achieve through prescriptive legal measures, such as those possible through contracts or privacy agreements. Even if the users were able to afford the costs of transparency, and give informed consent for the use of their data, the changing nature of technology would still leave the door open for privacy harms and opportunism by those who want to cause these privacy harms. As discussed earlier, fiduciary law, as opposed to contracts, affords the kind of deliberative and strategic interaction required to guard against the opportunists. Privacy is contextual, and depends on multiple factors, such as the nature of information, the context it is shared in, prospective users of that information, etc. (Nissenbaum 2011; Solove 2007). Fiduciary law allows for the flexibility required to cater to the contextual nature of privacy. Here, I will use security, anonymization and data minimization as examples of contextualization and flexibility required to deal with privacy issues. These, however, are just examples, and not an exhaustive list of cases where decisions and methods for privacy protection require contextualization.

Securing user data, an integral aspect of privacy protection, requires diligence and regular upgrading of security measures against cyberattacks and hacks. The recent case of the cyberattacks on the UK's National Health Service computers with the ransomware WannaCry is a case in point (Martin et al. 2017). Systems were largely found vulnerable because of a failure to upgrade software, rendering them unable to cope up with the ransomware (Martin et al. 2017). Health data, as discussed before, is particularly valuable to cyber attackers and healthcare is, therefore, one of the most targeted sectors in terms of cyberattacks (Athinaiou 2017; Martin et al. 2017). Securing health data, thus, requires diligent measures, which can guard against an opportunist hacker who may exploit vulnerabilities in a digital system. Data security may also require some secrecy or incomplete disclosure of data security policies (to keep them secret from hackers, for example). It can be difficult to counter such opportunism through use of contracts which specify what steps health data controllers need to take to secure user data, as it will be hard to anticipate all future contingencies (such as new tools for hackers or changes in security technologies). Fiduciary law, on the other hand, because of its open-ended approach and deliberative requirements (through the duty of loyalty) can be helpful in ensuring that health data controllers take appropriate measures to secure user health data. Fiduciary law can also help increase data sharing by not prescribing expansive security requirements for controllers who are collecting less sensitive or easily securable data.

Another crucial aspect of privacy protection for electronic data is anonymization (Ohm 2009). Anonymization aims to make re-identification of data subjects impossible, such that data can be shared for useful purposes, in an aggregated form, without the risks of privacy harms. The importance of anonymization or de-identification (either one or both), has also been recognized in and embedded into legislation, such as through the European Union's GDPR and HIPAA

in the United States (Hintze 2017; Yakowitz 2011). These laws often prescribe techniques for anonymization, such as removal of personal identifiers (such as names, phone numbers, social security numbers, etc.) (Ohm 2009; Yakowitz 2011). However, recent studies have shown that such prescriptive techniques may not be adequate, as computer scientists were able to re-identify individuals from anonymized data stripped of personal identifiers (Narayanan and Felten 2014; Ohm 2009). Stringent anonymization may therefore, require contextualization such that data is also stripped of indirect identifiers or is randomized, depending upon the kind of data that is collected (Ohm 2009). Further, the risk of re-identification may not be the same for all kinds of data, and for some data, it may be enough to apply techniques that make re-identification complex enough to take away the incentives for re-identification (Yakowitz 2011).

Another problem with prescribing anonymization through legal measures is that anonymization may not even be desirable for some kinds of data. Evans (2011) points out that anonymization may render linking data longitudinally impossible. Longitudinal health data, collected across different health environments, can be invaluable in generating insights for an individual as well as on a more general level, for example, by helping researchers determine the correlations between different biological factors and enable more organized efforts to tackle health and social problems (Evans 2011; Holman et al. 2008). Requiring anonymization for all health data may take away the opportunity to assemble longitudinal data for research as well as for other uses wherein the data subject may benefit without serious threats to their privacy.

Thus, as in the case of securing user data, anonymization too requires contextual decision making. Such contextual decisions can be hard to codify in the form of contracts, which would have to anticipate all future contingencies in all possible contexts. As fiduciaries, digital health data controllers would be able to make contextual decisions about anonymization, where they can decide whether or not anonymization is needed, and to what degree.

Finally, as a third example of the advantages of a contextual approach to privacy, consider data minimization. Data minimization as a principle has also been included in the GDPR and states that data must be "limited to what is necessary in relation to the purposes for which they are processed" (Art. 5 GDPR n.d.). In addition to the scope of data collected, the minimization principle within GDPR also relates to the time for which it is retained and stored (Recital 39 n.d.; Zarsky 2016). The minimization principle can be important in protecting user privacy by limiting the opportunities for collecting irrelevant data as well as minimizing cyber security risks by requiring controllers to delete data when no use is intended. However, in the age of big data analytics, an ex-ante analysis of the relevance of data and restrictions on its retention can severely limit the benefits of big data analytics. This has also been noted by other commentators [see Zarsky (2016)] while some have also predicted that a requirement such as data minimization is likely to be breached (Rubinstein 2012)[8]. Again, a contextual approach to privacy, as made possible through a fiduciary approach, can achieve a better balance between privacy protection and achieving benefits of big data analytics, by loosening the data minimization or replacing it by achieving the intended effects of minimization through other means wherever necessary. While contractual law and statutory law (such as GDPR) also can (and do, in case of GDPR[9]) have context-sensitive features, a fiduciary approach can enable more flexibility in fulfilling data controllers' obligation of protecting user privacy, particularly in allowing data controllers to choose the most appropriate method of doing so while ignoring recommendations that may be counter-intuitive or disadvantageous in the given context.

Further, as fiduciaries, digital health data controllers would not only be required to take a contextual approach to privacy protection, but also not deceive or actively harm the data subject in pursuing their obligation to protect the privacy of data subjects. This is an advantage over contract or statutory law, which may leave room for opportunistic or deceptive behavior on part of data controllers [see for example Wachter (2018) and Zarsky (2016) for examples of loopholes in GDPR which data controllers might use for their benefit and which may deny rights to data subjects exposing them to risks].

Here, I have outlined how fiduciary relationships between health data subjects and health data controllers can enable collective participation by ensuring better decisions are made concerning data on behalf of the users. Fiduciary relationships not only compensate for the high costs of transparency, but are also better suited than alternative approaches as they can flexibly contextualize privacy (and privacy protection).

[8] GDPR does allow some exceptions for application of the minimization principle, but these exceptions also have problems and may not be applicable for a variety of big data analyses [see Zarsky (2016) for a more detailed discussion of limits of data minimization principle as included in the GDPR].

[9] For example, Article 25 (GDPR—Data protection by design and by default n.d.) states that data controllers should take into account "state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons" in determining the appropriate measures in implementing privacy by design.

Nature and scope of duties and obligations that health data controllers should have as fiduciaries

As argued in "The nature and scope of fiduciary duties" section, central to fiduciary law is the duty of loyalty, which primarily dictates that fiduciaries must keep the interests of the beneficiaries at the forefront. Yet, as argued earlier, scholars and courts do not share a consensus on the scope of such a duty, that is, how far should the fiduciaries go in pursuit of beneficiaries' interest. The duty of loyalty can range, for example, from avoiding conflict of interest to an affirmative devotion towards the beneficiary.

The abstract and open-ended nature of fiduciary duty of loyalty, however, as I argued earlier, does not render it an empty vessel. Rather, it opens up the possibility for pluralism within fiduciary law and for more precise formulations of specific fiduciary relationships. At the same time, if the duty is too expansive, within a specific fiduciary relationship, then the duty will be too difficult to carry out. The open-ended and abstract nature of fiduciary duty, therefore, needs to be balanced with specificity about the interests of the beneficiary that the fiduciary should pursue within a specific fiduciary relationship.

The proposal that we specify the scope of fiduciary duty, such that there are bounds to fiduciary loyalty, is not unique and is also applied to traditional fiduciaries. For example, physicians are not expected to be loyal to their patients at all costs. A physician, for example, is only obligated to provide care to a patient at a reasonable time and place (for instance, a physician is not obligated to attend to night or house calls) (Mehlman 2015).

Courts also recognize similar limits to the degree of loyalty physicians owe to their patients. That is, while the physician is expected to keep the patient's interest ahead of his own interest, courts recognize that there should be reasonable limits to the expectation of such loyalty from the physician. For example, while physicians cannot deny treatment pending assurance of payment in urgent situations, they may terminate their relationship unilaterally (even on financial grounds) with the patient as long as the patient is given notice and reasonable opportunity to get treatment elsewhere (Mehlman 2015).

It is therefore, important to specify the bounds of fiduciary duty that health data controllers have towards their data subjects. First, as an essential part of the duty of loyalty, health data controllers should not use information collected by them to harm individuals, for example, by harassing, exploiting, embarrassing or manipulating them. Beyond this primary requirement, I argue here that the duty of loyalty for health data controllers should be specifically about the protection of privacy of the users sharing their health data. Catering to individual privacy concerns is an important step in enabling trust within the users to share their data, and thus, opening the way for collective participation in the digital health revolution. As argued, in the previous section, privacy protection requires contextualization, wherein the type of data as well as the technologies involved in the collection, storage and sharing are taken into consideration. The duty of loyalty, aimed specifically at protecting the privacy of users, thus, still requires deliberation and diligence on the part of health data controllers.

At the same time, defining the duty of loyalty as specifically aimed at privacy protection avoids the danger of making the duty too expansive, and the corresponding difficulties of carrying out such a duty. An expansive duty of loyalty, such as one requiring a general affirmative devotion to the user, might take away the incentive for health data controllers to invest in digital health technologies, and thus, hamper the path towards a better healthcare system.

For example, an alternative possibility to the scope of fiduciary loyalty proposed here, would be to require that fiduciaries go beyond protection of privacy, and also ensure that a broader or general set of interests of the users are kept at the forefront when sharing health data with third parties, even in anonymized and de-identified form. This would, for example, require that data is shared only for purposes that are beneficial to the users. Such an expansive requirement, however, would put too much burden on health data controllers to evaluate the outcomes of the data shared by them with the third parties. It would also significantly reduce the incentive for health data controllers to share data, even in an anonymized form, for health research, as that might open up a possibility for claims of a breach by users who may not find the aim or outcomes of the research in their interests. This is not to argue that health data controllers should be allowed to share data with any third party. Rather, the lawful basis of sharing data with third parties should not be determined solely through fiduciary duties (which could lead to a more abstract and expansive definition of fiduciary duties), but also through legal instruments such as those already implemented (Long 2017).

Fiduciary breach vs medical malpractice

In the previous part of this section, I claimed that health data controllers themselves should not use information collected by them to harm individuals, for example, by harassing, embarrassing or manipulating them. Not causing harm to the beneficiary is an essential part of fiduciary duty and without such a requirement, users would not be able to trust the health data controllers, even if they are assured that their data would not be shared with third parties in an identifiable form. However, I claim here that a distinction should be made between harms caused by medical advice provided by health data controllers and other harms where health data controllers use the

data provided by users against them (for example, to harass, manipulate or embarrass them). Harms caused by medical advice by health data controllers, I argue, should be classified as medical malpractice, similar to how the law treats harmful or bad medical advice by physicians. In the following paragraphs, I provide the arguments for why such a distinction should be made and in particular, why the distinction is important for the future of digital health.

With the use of big data and machine learning algorithms, digital health apps not only collect and monitor health data but also offer personalized advice to the users (Higgins 2016). This phenomenon of impending reliance upon machine learning algorithms for health advice (as well as diagnosis and treatments) is referred to as "black-box" medicine (Ford and Price 2016). A key feature of black-box medicine is its opacity, as the amount of data involved and the complexity of algorithms, make it hard for humans to know exactly how the algorithms work (Ford and Price 2016).

The algorithms involved in black-box medicine rely upon using machine learning techniques to find underlying patterns in a large quantity of data. The large datasets required for accurate algorithms, however, will take time to assemble, and in the early stages of black-box medicine, as we stand now, these algorithms maybe prone to errors (Price 2017a). These errors demand a careful set of regulations and legal instruments to protect the users, and this has attracted the attention of regulatory bodies in the developed world, such as the Food and Drug Administration (FDA) in the United States (Price 2017b).

Regulating black-box medicine, however, can be quite challenging and there are risks involved in both, under-regulation and overregulation (Price 2017b)[10]. While under-regulation runs the risk of leaving the users exposed and vulnerable to medical harms, the risks of over-regulation come in the form of cost to innovation (Price 2017b). Requiring strict criteria for verification of black box algorithms may significantly increase the hurdles to get such products to the market, and thus, forestall the possibility of algorithmic medicine to improve the health care system. Further, verification of algorithms used in black-box is difficult in most cases, and even impossible in some (Ford and Price 2016)[11].

While fiduciary law could be used to force health data controllers to take steps to design error free algorithms, such a move may not only disincentivise investment into digital health technologies, it may also be impractical. The risk of being found guilty of a fiduciary breach may force companies to abandon algorithmic medicine, as guaranteeing an error free algorithm may not be possible. Further, there is also a risk that users may claim a fiduciary breach (on account of a health data controller not being loyal) even when there is no harm or when the degree of harm is too small. The argument here is not that health data controllers should not be held accountable for the algorithms they develop and use, rather that the harms caused by those algorithms, in the medical context, should be treated similar to medical malpractice and resolved through other legal instruments. Price (2017a), for example, argues that laws such as medical liability litigation can and should be used for accountability of algorithmic medicine.

Again, the proposal to make a distinction between fiduciary harms and medical malpractice is not unique to algorithmic medicine. The said distinction is also applicable, under current law, for physicians (Mehlman 2015). Courts make a distinction between medical malpractice and fiduciary harms caused to the patient. For injuries caused by sub-standard care (including wrong or bad medical advice), as well as to deter unreasonable or unprofessional behavior by physicians, medical liability law is applied, with physicians being tried for medical malpractice (Mehlman 2015; Price 2017a). In contrast, fiduciary law is usually reserved for protection of patient confidentiality and for rare cases of physicians' acting purely out of self-interest (Drozd and Dale 2006; Mehlman 2015).

As I have discussed through this paper, fiduciary law is abstract and open-ended. Applying fiduciary law to regulate algorithmic medicine would be detrimental for the progress of and innovation within the field of algorithmic medicine, which at least in theory, and with other instruments of regulation, can have significant positive effects on the state of healthcare. The scope of fiduciary duties for data health controllers defined here attempts to find a balance between protecting individual interests, by addressing privacy concerns, and collective interests of getting valuable insights about human health as well as well as facilitation of research and innovation required for gathering such insights.

Finally, it should be noted that although through this section I have tried to specify the bounds of fiduciary duty of

[10] For a more detailed overview of current approaches to regulation of algorithmic medicine, see (Price 2017b).

[11] (Ford and Price 2016) suggest two main ways for verifying algorithms used in Black-box medicine: clinical trials and computational verification. Both methods come with enormous practical challenges. In the case of computation verification, most regulating bodies aren't equipped with expertise to carry out such a verification. While independent third parties might compensate for the lack of expertise, it would require significant compensation for third parties to offer their expertise. Further, for a comprehensive verification, third parties would require a broad access to data used to develop algorithms, which may open further concerns about privacy of the users. Clinical trials, on the other hand, are slow and expensive, and in most cases would only offer a small benefit. See (Ford and Price 2016) for a more detailed overview.

loyalty, the courts would have an important role in contextual interpretations of these bounds, and in deciding whether a fiduciary breach has taken place or not. This is not a limitation, but rather an important aspect of fiduciary law, which can push the fiduciary to go beyond what can be defined by contractual law in protecting the interests of the beneficiary. As discussed in an earlier example, fiduciary duties are better suited than statutory or contractual obligations to ensure that health data controllers take appropriate data security measures to protect user data from hackers. At the same time, data breaches may happen due to happen vulnerabilities beyond the control of health data controllers[12], leaving it upon courts to decide whether, for a particular case, the security breach also amounts to a fiduciary breach or not.

Gaps in and limits of fiduciary law

While the application of information fiduciary status to health data controllers will address user concerns about privacy when sharing health data with digital health data controllers, there are other problems that remain unsolved with this proposal and would need to be addressed by other methods. For instance, there is a threat that creation of health data repositories by private entities may lead to "commercialization of science", and dilution of principles of scientific integrity as research moves from universities to private companies (Sharon 2016).There is also no guarantee that markets will lead to sharing of this data with third parties that can advance the state of healthcare for the society as a whole. There is a possibility, for example, that owing to economic inequalities, use of such devices, and hence, collection of data, may be limited to an economically privileged section of society, which may further escalate inequalities in health care delivery as well as create population biases when, and if, such data is used for purposes such as drug discovery or disease diagnosis (Sharon 2016).

One challenge for the proposal to give information fiduciary status to health data controllers is the diverse nature of legal systems and regulations across the globe. In an inter-connected digital world, where the data can move easily across borders, this is a challenge for most data regulation policies (Bu-Pasha 2017). The unique challenge for the proposal to have fiduciary relationships between health data controllers and data-subjects, however, is that fiduciary law is explicitly defined in only a few legal systems, in particular in systems of common law tradition (for example, in legal systems of countries such as USA, Australia, England, Canada) (Gelter and Helleringer 2018). By contrast, civil law jurisdictions, such as in countries in continental Europe, fiduciary duties or relationships are not explicitly defined (Gelter and Helleringer 2018). Yet, as Gelter and Helleringer (2018) have argued, there are implicit fiduciary principles within civil law systems and in some domains, civil law jurisdictions have even added fiduciary equivalents to existing law. The aim of this paper has to been to argue for fiduciary principles—in particular, the duty of the fiduciary to keep the interests of beneficiaries at the forefront through deliberation and diligence—to deal with privacy issues concerning health data. Since there are provisions within civil law systems that are principally similar to fiduciary law, an absence of explicit fiduciary law would not be a major constraint in adopting the principles argued for in the paper. Yet, future work in legal scholarship is needed to sketch out the details of this proposal, bearing in mind the challenge brought forth by the movement of data across legal regimes.

In the previous section, I also pointed out the challenge in defining health data, and therefore, digital health data controllers. I argued that fiduciary duties should be imposed only on digital health data controllers who (a) Process data with the intention of using the data to determine the health status of a specific person, or (b) Process raw data in situations where it will be reasonable for a data subject to conclude that the data is being collected to determine their health status. These criteria are important to reach a balance where the scope of data controllers with fiduciary obligations is not too expansive, while sensitive health data is still protected. While the criteria I propose may achieve this balance principally, there is more work required to define these criteria in a legally pragmatic way.

Further, there are permissible latitudes within the fiduciary law which leave open the possibility of exploitation. For example, physicians can breach patient confidentiality to protect public health (Mehlman 2015). There are also exceptions to lawyer's fiduciary duty to their clients, and the attorney-client privilege which protects the client's information. Governments, for example, may use such latitudes and exceptions within fiduciary law, by forcing health data controllers to share information with them on grounds of public safety. Governments have made similar claims in the past, mandating access to digital data, which has led to mass surveillance on the grounds of public safety (Abelson et al. 2015). So, it should be emphasized that this paper is not an argument to abandon the ambitions for more transparency and accountability when dealing with health data controllers, as they can help in enabling increase literacy of citizens about issues related to privacy enabling a more democratic governance of digital tools and healthcare system as a whole. The limits of and gaps in the fiduciary law I have pointed

[12] For example, cyber-attacks may exploit what are known as "Zero-day" vulnerabilities which haven't been discovered yet, even by the vendors of the software (with such vulnerabilities) (Kumar 2014). Similarly, cyber-attacks maybe carried out through non-technical means, such as by gaining physical access to network systems through use of force or physical attacks (Byres et al. 2004).

out above are a testimony to the fact that my proposed solution can only take us so far. It also reminds us that we, as members of society, must continue to ask questions about our rights to fair treatment and the ethical conduct owed to us by those involved in the collection, use, analysis, distribution, and sale of our personal data.

Conclusion

Digital health technologies have the potential to transform healthcare by helping individuals live healthier lives as well as by providing valuable insights into our health as a collective. This potential revolution, enabled by collection, use, and analysis of large amounts of health data, however, requires collective participation and poses threats to the individuals, exposing intimate information to privacy related harms. In this paper, I have argued that transparency mechanisms do not adequately address individual privacy concerns, and thus, do not enable the trust required for collective participation.

To ensure the protection of privacy of users sharing health data, I have argued that the relationship between users sharing health data and digital health data controllers should be recognized as a fiduciary relationship, such that health data controllers would keep the interests of the users at the forefront. The relationship between health data controllers and users shares characteristics with traditional fiduciary relationships and involves similar circumstances as those under which traditional fiduciary relationships are recognized. A fiduciary relationship between health data controllers and users is also better suited than alternative approaches for protecting user privacy and thus, enabling users to trust data controllers with their health data.

Acknowledgements I would like to thank Elizabeth O' Neill, Anthonie Meijers, Claudia-Melania Chituc, John Danaher, Tamar Sharon, Linnet Taylor and two anonymous reviewers for their immensely valuable and helpful comments on earlier drafts of this article.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

References

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., et al. Weitzner, D. J. (2015). Keys under doormats: Mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity, 1*(1), 69–79. https://doi.org/10.1093/cybsec/tyv009.

Acquisti, A., Adjerid, I., & Brandimarte, L. (2013). Gone in 15s: The limits of privacy transparency and control. *IEEE Security Privacy, 11*(4), 72–74. https://doi.org/10.1109/MSP.2013.86.

Adjerid, I., Acquisti, A., Brandimarte, L., & Loewenstein, G. (2013). Sleights of privacy: framing, disclosures, and the limits of transparency. In *Proceedings of the ninth symposium on usable privacy and security* (pp. 9:1–9:11). New York, NY: ACM. https://doi.org/10.1145/2501604.2501613.

Art. 5 GDPR—Principles relating to processing of personal data. (n.d.). Retrieved December 13, 2018 from https://gdpr-info.eu/art-5-gdpr/.

Art. 12 GDPR. (n.d.). Retrieved February 6, 2018 from https://gdpr-info.eu/art-12-gdpr/.

Art. 25 GDPR—Data protection by design and by default. (n.d.). Retrieved December 19, 2018 from https://gdpr-info.eu/art-25-gdpr/.

Article 29 Working Party. (2015). *ANNEX—health data in apps and devices*. Retrieved February 8, 2018 from http://webcache.googleusercontent.com/search?q=cache:MlBCtv-DN6gJ:ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf+&cd=1&hl=en&ct=clnk&gl=nl&client=firefox-b-ab.

Athinaiou, M. (2017, July 17). *Why has healthcare become such a target for cyber-attackers?* Retrieved August 28, 2018 from http://theconversation.com/why-has-healthcare-become-such-a-target-for-cyber-attackers-80656.

Balkin, J. (2014, May 3). Balkinization: Information fiduciaries in the digital age. Retrieved October 31, 2017 from https://balkin.blogspot.nl/2014/03/information-fiduciaries-in-digital-age.html.

Balkin, J. M. (2015). Information fiduciaries and the first amendment. *U.C. Davis Law Review, 49*, 1183.

Barocas, S., & Nissenbaum, H. (2009). *On notice: The trouble with notice and consent* (SSRN Scholarly Paper No. ID 2567409). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=2567409.

Brennan-Marquez, K. (2015). Fourth amendment fiduciaries. *Fordham Law Review, 84*, 611.

Brinig, M. F. (2011). *Parents, trusted but not trustees or (Foster) parents as Fiduciaries* (SSRN Scholarly Paper No. ID 1767412). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=1767412.

Bu-Pasha, S. (2017). Cross-border issues under EU data protection law with regards to personal data protection. *Information and Communications Technology Law, 26*(3), 213–228. https://doi.org/10.1080/13600834.2017.1330740.

Byres, E. J., Franz, M., & Miller, D. (2004). The use of attack trees in assessing vulnerabilities in scada systems. In *IEEE conference international infrastructure survivability workshop (IISW'04). Institute for Electrical and Electronics Engineers*.

Bywater, A., & Armstrong, J. (2015, March 6). *EU health data definition concerning lifestyle and wellbeing apps*. Retrieved February 8, 2018 from http://www.corderycompliance.com/eu-health-data-definition-concerning-lifestyle-and-wellbeing-apps/.

Candeub, A. (2013). Transparency in the administrative state. *Houston Law Review, 51*, 385.

Cestui que trust. (2006). Retrieved December 4, 2017 from https://legal-dictionary.thefreedictionary.com/cestui+que+trust.

Crawford, K., Lingel, J., & Karppi, T. (2015). Our metrics, ourselves: A hundred years of self-tracking from the weight scale to the wrist wearable device. *European Journal of Cultural Studies, 18*(4–5), 479–496. https://doi.org/10.1177/1367549415584857.

Dobbs, D. (2008). *Law of torts (hornbook series)*. Eagan: West Academic.

Drozd, S., & Dale, R. (2006, March 27). *General principles of medical malpractice litigation*. Lerners Lawyers. Retrieved from http://www.lerners.ca/lernx/general-principles-of-medical-malpractice-litigation/.

Evans, B. J. (2011). Much ado about data ownership. *Harvard Journal of Law & Technology, 25*, 69.

Farrell, H. M. (2012). Transparency in psychiatric care. *Asian Journal of Psychiatry, 5*(3), 273–274. https://doi.org/10.1016/j.ajp.2012.07.011.

Fitbit Privacy Policy. (2016). Retrieved October 5, 2017 from https://www.fitbit.com/nl/legal/privacy.

Ford, R. A., & Price, W. N. I. (2016). Privacy and accountability in black-box medicine. *Michigan Telecommunications and Technology Law Review, 23*, 1.

Frankel, T. T. (2010). *Fiduciary law*. Oxford: Oxford University Press.

Gelter, M., & Helleringer, G. (2018). *Fiduciary principles in European Civil Law Systems* (SSRN Scholarly Paper No. ID 3142202). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=3142202.

Gold, A. S. (2013). *The loyalties of Fiduciary law* (SSRN Scholarly Paper No. ID 2370598). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=2370598.

Gostin, L. O., & Hodge, J. G. J. (2001). Personal privacy and common goods: A framework for balancing under the national health information privacy rule. *Minnesota Law Review, 86*, 1439.

Guerin v. The Queen, 2 SCR 335 (C 1984). Retrieved from http://canlii.ca/t/1lpfn.

Higgins, J. P. (2016). Smartphone applications for patients' health and fitness. *The American Journal of Medicine, 129*(1), 11–19. https://doi.org/10.1016/j.amjmed.2015.05.038.

Hintze, M. (2017). *Viewing the GDPR through a de-Identification Lens: A tool for compliance, clarification, and consistency* (SSRN Scholarly Paper No. ID 2909121). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=2909121.

Holman, C. D., Bass, A. J., Rosman, D. L., Smith, M. B., Semmens, J. B., Glasson, E. J., et al. Stanley, F. J. (2008). A decade of data linkage in Western Australia: Strategic design, applications and benefits of the WA data linkage system. *Australian Health Review: A Publication of the Australian Hospital Association, 32*(4), 766–777. https://doi.org/10.1071/AH080766.

Jensen, C., & Potts, C. (2004). Privacy policies as decision-making tools: An evaluation of online privacy notices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 471–478). New York, NY: ACM. https://doi.org/10.1145/985692.985752.

Johnson, L. (2003). After enron: Remembering loyalty discourse in corporate law. *Delaware Journal of Corporate Law, 28*, 27.

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica, 47*(2), 263–291. https://doi.org/10.2307/1914185.

Kaplan, B. (2016). How should health data be used? Privacy, secondary use, and big data sales. *Cambridge Quarterly of Healthcare Ethics, 25*(2), 312–329. https://doi.org/10.1017/S0963180115000614.

Konnoth, C. (2015). Classification and standards for health information: ethical and practical approaches. *Washington and Lee Law Review Online, 72*, 397.

Kumar, A. (2014). *Zero day exploit* (SSRN Scholarly Paper No. ID 2378317). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=2378317.

Licht, A. N. (2016). *Motivation, information, negotiation: Why fiduciary accountability cannot be negotiable* (SSRN Scholarly Paper No. ID 2811237). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=2811237.

Long, B. (2017, April 11). Lewis silkin—introductory guide to data sharing. Retrieved October 4, 2017 from http://www.lewissilkin.com/Insights/Introductory-guide-to-data-sharing.

Lupton, D. (2015). *Digital health technologies and digital data: New ways of monitoring, measuring and commodifying human embodiment, health and illness* (SSRN Scholarly Paper No. ID 2552998). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=2552998.

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: how safe are we? *BMJ, 358*.

McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *I/S: A. Journal of Law and Policy for the Information Society, 4*, 543.

Mehlman, M. J. (2015). Why physicians are fiduciaries for their patients. *Indiana Health Law Review, 12*(1), 1–64. https://doi.org/10.18060/18959.

Miller, P. (2011). A theory of fiduciary liability. *McGill Law Journal/Revue de Droit de McGill, 56*(2), 235–288. https://doi.org/10.7202/1002367ar.

Narayanan, A., & Felten, E. (2014, July 9). *No silver bullet: De-identification still doesn't work*. Retrieved from http://www.privacylives.com/wp-content/uploads/2015/02/narayanan-felten-no-silver-bullet-de-identification-2014.pdf.

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus, 140*(4), 32–48. https://doi.org/10.1162/DAED_a_00113.

Ohm, P. (2009). *Broken promises of privacy: Responding to the surprising failure of anonymization* (SSRN Scholarly Paper No. ID 1450006). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=1450006.

Patil, S., Patruni, B., Lu, H., Dunkerley, F., Fox, J., Potoglou, D., & Robinson, N. (2015). *Privacy of health records: Europeans' preferences on electronic health data storage and sharing*. Santa Monica: Rand Corporation.

Price, W. N. (2017a). *Medical malpractice and black-box medicine* (SSRN Scholarly Paper No. ID 2910417). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=2910417.

Price, W. N. (2017b). *Regulating black-box medicine* (SSRN Scholarly Paper No. ID 2938391). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=2938391.

Recital 39—Principles of data processing. (n.d.). Retrieved December 13, 2018 from https://gdpr-info.eu/recitals/no-39/.

Recital 58, GDPR. (n.d.). Retrieved February 6, 2018 from https://gdpr-info.eu/recitals/no-58/.

Rotman, L. (2011). Fiduciary Law's 'Holy Grail': Reconciling theory and practice in fiduciary jurisprudence. *Knowledge@SchulichLaw, 0*(0). Retrieved from https://ojs.library.dal.ca/KNOWSL/article/view/4742.

Rubinstein, I. (2012). *Big data: The end of privacy or a new beginning?* (SSRN Scholarly Paper No. ID 2157659). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=2157659.

Sharon, T. (2016). The Googlization of health research: From disruptive innovation to disruptive ethics. *Personalized Medicine, 13*(6), 563–574. https://doi.org/10.2217/pme-2016-0057.

Sitkoff, R. H. (2011). The economic structure of Fiduciary law. *Boston University Law Review, 91*, 1039.

Smith, D. G. (2002). The critical resource theory of Fiduciary duty. *Vanderbilt Law Review, 55*, 1399.

Smith, H. E. (2013). *Why Fiduciary law is equitable* (SSRN Scholarly Paper No. ID 2321315). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=2321315.

Solove, D. J. (2007). I've got nothing to hide and other misunderstandings of privacy. *San Diego Law Review, 44*, 745.

Spagnuelo, D., & Lenzini, G. (2016). Patient-centred transparency requirements for medical data sharing systems. In *New advances in information systems and technologies* (pp. 1073–1083). Cham: Springer. https://doi.org/10.1007/978-3-319-31232-3_102.

Terry, N. (2012). *Protecting patient privacy in the age of big data* (SSRN Scholarly Paper No. ID 2153269). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=2153269.

The Seven-Per-Cent Solution. (1976). Universal Studios.

Wachter, S. (2018). The GDPR and the internet of things: A three-step transparency model. *Law, Innovation and Technology, 10*(2), 266–294. https://doi.org/10.1080/17579961.2018.1527479.

Williamson, O. E. (1975). *Markets and hierarchies: Analysis and antitrust implications: A study in the economics of internal organization* (SSRN Scholarly Paper No. ID 1496220). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=1496220.

Worthington, S. (2006). *Equity*. Oxford: OUP Oxford.

Yakowitz, J. (2011). Tragedy of the data commons. *Harvard Journal of Law & Technology, 25*, 1.

Zarsky, T. Z. (2016). Incompatible: The GDPR in the age of big data. *Seton Hall Law Review, 47*, 995.

Zittrain, J., & Balkin, J. M. (2016, October 3). *A grand bargain to make tech companies trustworthy. The Atlantic*. Retrieved from https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/.