Good science at heart

Lessons on ethics from big data research in sudden cardiac arrest

Bak, M.A.R.

Publication date
2021

11 | Towards trust-based governance of health data research: a European case study

"It is said that the doorkeeper does not know the interior of the law but only the path he must constantly patrol outside of the entrance."
(Franz Kafka, *The Trial*. 1925; p. 198)

Summary[i]

Developments in medical big data analytics may bring societal benefits but are also challenging privacy and other ethical values. At the same time, an overly restrictive data protection regime can form a serious threat to valuable observational studies. Discussions about whether data privacy or data solidarity should be the foundational value of research policies, have remained unresolved. This dilemma was the starting point for our case study on the implementation of the General Data Protection Regulation (GDPR) within a European research consortium. We found a gap between the aims of the regulation and its effects in practice. First, strictly formalised data protection requirements may cause routinisation among researchers instead of substantive ethical reflection. Second, harmonisation across Europe and data sharing between countries is hampered by different interpretations of the law, which stem at least to a certain extent from different views about ethical values. Third, strong enforcement may actually crowd out trust between actors in the health data research ecosystem. Building on this case study, we argue that the concept of trust provides a more useful frame for data governance than the privacy-solidarity debate. The paper details three aspects of trust that can help to create a responsible research environment: trust as multi-agent concept; trust as a rational and democratic value; and trust as method for priority setting. Mutual cooperation in research – among researchers and with data subjects – is very much grounded in trust, which should be more explicitly embedded in the governance of health data research.

[i] This chapter was submitted for publication as: Bak MAR, Tan HL, Ploem MC, Blom MT, Willems DL. Towards trust-based governance of health data research: a European case study. *Medicine, Health Care and Philosophy*. 2021; under review.

11.1 Introduction

With the rise of computerised databases, privacy in relation to information technology has been a subject of societal debate for about half a century now. In medicine, a duty of confidentiality was already included in the ancient Hippocratic Oath: "What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men [persons], which on no account one must spread abroad, I will keep to myself".[1] This duty exists to safeguard access to health care and to protect individual patients' privacy. The concept of privacy is a social construction and difficult to define: no single objective or judicial definition may suffice to describe the lived experiences of privacy across contexts.[2] Most authors agree, however, that we can distinguish between physical (bodily seclusion), proprietary (things like identity and name), and informational (personal data) privacy.[3] The latter is our concern in this article.

Informational privacy in health care and research is currently being challenged by the increased globalization that stimulates information sharing and produces a growing number of international research consortia, as well as by technological developments like *big data* and *machine learning* that are known to exacerbate existing privacy risks and to create new ones.[4,5] The era of big data enables a realisation of personalised or precision medicine that uses networked resources to combine all kinds of information (e.g. health records, biospecimen, socio-economic and behavioural data) in order to tailor prevention and treatment to the individual patient.[6] These linkages of data and the scale of aggregation create the potential for misuses and discrimination, e.g. in terms of state surveillance or companies denying insurance coverage based on risk profiles.[7,8] Some scholars have suggested, using Jeremy Bentham's idea of the panoptic prison where prisoners can be unknowingly observed at all times, that we are moving towards an "informational panopticon".[9] Others believe that personal data are becoming 'overprotected' in response to growing privacy concerns. A number of scientists have argued that data protection laws in the European Union (EU) may harm public well-being by hampering progress in health data research.[10-11]

Should we let informational self-determination prevail over data sharing for public health benefit or *vice versa*? In this article we explore another way out of this dilemma: one of trust. The concept of trust stands at the core of health data research but lacks a philosophical underpinning in this context. We make use of an ethical-empirical approach to analyse researchers' lived experiences with data protection rules, which highlights the limits of data protection legislation and the important role for trust. The structure of the paper is as follows. First, we describe the current status of the ethical debate on governance of health data research, including the legal background. Second, we present our case study of a European research consortium that uses an international 'big' database to study a particularly vulnerable group of patients

(namely, victims of sudden cardiac arrest [SCA], a life-threatening condition). We reflect on practice by comparing researchers' experiences with the aims of the European Union's General Data Protection Regulation (GDPR). Third, we propose three 'rational' characteristics of trust that can be utilised by researchers and policymakers to promote responsible health data research. The paper concludes with final remarks and suggestions for further study.

11.2 Background on governance of health data research

The term governance has the same origin as the prefix 'cyber': both stem from the Greek word *κυβερνήτης* (kybernetes, translation: steersperson of a ship) that was first used by Plato to describe a person governing a state.[12] Data governance refers to the making of arrangements for responsible collection, storage, usage and sharing of personal data and is needed to account for ethical concerns arising from the use of health-related data, especially when collaborating in large-scale research projects.[13] Governance of health data research has become more important in recent decades as researchers gather data from many sources to create clinical, genetic and socio-economic profiles of data subjects. The growing technological possibilities for big data analytics and the corresponding potential for misuses, have led to a heightened sensitivity for privacy concerns rooted in individual autonomy. At the same time, technology can make some values and norms easier to realize: it supplies new 'cans' which result in new 'oughts'. The can of big data may create a new ought of solidarity in data sharing for public health research. We discuss these two perspectives hereafter, before linking the debate to the EU legal framework.

11.2.1 Privacy versus solidarity

On one side, there is a trend of informational privacy becoming increasingly important. This trend can be put in instrumental terms of preventing harms to data subjects and in principled terms of respecting subjects' autonomy and human dignity.[14] While there are national and cultural differences in research ethics approaches,[15] the general tendency since the Nuremberg trials has been to increasingly view the autonomy of research subjects as the most fundamental value in research ethics.[16,17] Increased attention for informational privacy also follows from more recent controversies in health data research, such as the issues around informed consent during the creation of national health databases in the United Kingdom and Iceland.[18,19] As health researchers are forming partnerships with companies, people experience an increasing loss of control over their personal data.[20,21] These privacy concerns are accelerated by the rise of what Zuboff and others before her have called 'surveillance capitalism': data misuses by large internet companies (e.g. Google DeepMind and Facebook/Cambridge Analytica).[22]

Privacy can be defined in many different ways,[ii] but generally we are seeing that its meaning is changing under the pressure of new information technologies that enable large-scale data mining.[23] Anonymization of data may lead to unreliable results while it may not suffice to protect people's privacy in our increasingly networked society.[25,26] Recognizing the limits of anonymization, privacy is increasingly conceptualised as *control*, represented in formalised informed consent procedures and data access requirements (consider GDPR Recital 7: "Natural persons should have control of their own personal data"). While measures of control may be necessary, they are never sufficient. The burden of privacy should not be borne by individual data subjects, especially given the well-documented lack in understanding of their consent among people who donate data[27] and because privacy is about more than being able to say 'yes' or 'no'. It is also about how the data is used and by whom.[28] Accordingly, Bredenoord and colleagues criticise the 'consent or anonymise' approach and propose that we best protect people who donate data or tissue by reframing informed consent in terms of 'consent for governance', i.e. focused on research infrastructure rather than on study content.[29,30] While this is arguably what many research projects do already, the approach highlights well the limits of relying on consent alone and shows that (regardless of whether consent is needed) health data research *always* requires a protective layer of sharing agreements, ICT security, and potentially oversight by research ethics committees.[31]

The question is whether such a protective layer would be sufficient and abolishes the need for informed consent, in favour of public health. In response to legislative burdens of data protection, debates have started on whether *data solidarity* (i.e., supporting the health of future others by sharing one's personal data) rather than privacy would be the proper basis of health data research.[6] Proponents of this argument suggest that a 'neoliberal' focus on autonomy undermines social institutions, that the harm due to non-use of health data can be greater than harm from uses,[32,33] and that minimal risk research should not require consent.[34] They think that the possibilities that big data analytics provide, create an 'ought' for data sharing. In response to increasing individual freedoms and a declining feeling of community, a push for data solidarity mirrors what is arguably a 'communitarian turn' in bioethics.[35,36] We are currently seeing this in the response to the COVID-19 pandemic: when humans are suffering as a global sick body, some political actors think this creates priority for mass surveillance over individual privacy.[37;iii]

[ii] One influential definition of informational privacy was given by Westin: *"The claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others"*.[24]

[iii] See also: Yuval Noah Harari (20 March 2020), The world after coronavirus. Financial Times. [https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca7]

Political mentions of data solidarity were found across Europe already in the pre-pandemic era. One example is a letter to parliament by the then Minister for Medical Care in the Netherlands who characterised data as "the new social revolution" and argued that since the cost of the Dutch healthcare system is shared by all citizens, regardless of whether they need it, the same principle should be envisaged for data (p. 10).[38] In response, Dutch ethicists commented that solidarity is not without risks as personal data sharing limits self-determination and can contribute, for instance, to profiling based on lifestyle.[39] Political documents like this one generally remain vague about how privacy and solidarity are conceptualised but academia fares no better: while there is a blossoming scholarly literature on the concept of solidarity in relation to health data, there exists no consensus on how it should be defined, other than as something "contributing positively to the social fabric of society".[6,40] We are seeing a policy vacuum that is caused, at least in part, by a conceptual vacuum about the meaning of privacy and solidarity.[41] These concepts are difficult to define as they are very much linked: an autonomy-inspired striving for individual privacy paradoxically leads to more dependence on others; and individual benefits may give rise to group-level privacy harms.[42,43; iv]

11.2.2 Legal framework in the European Union: the GDPR

Just as information technology develops over time, legal documents are not set in stone. The increasing technological possibilities and international collaboration are reflected in the development of data protection legislation such as the GDPR which came into force in May 2018. In contrast with the 1995 Data Protection Directive, the new law is directly applicable in all EU Member States and applies to all EU citizens, no matter their location. It also updates the Directive by explicitly mentioning genetic data, and has a stronger focus on accountability and high fines for data breaches.[46] Along with national laws that specifically govern the health care sphere (e.g. rules about medical confidentiality), the GDPR aims to protect data privacy through various principles and through practical requirements such as the mandatory conducting of a Data Protection Impact Assessment (DPIA) for large-scale health datasets. It is based on two legal rights that overlap: namely, the right to data protection which is grounded in the broader right to privacy. Researchers including the ones we spoke with, often refer to data protection as a moving target and highlight

[iv] Adequately protecting health databases, for instance, is impossible without involving ICT security experts. Or consider the individual cardiac arrest survivor who benefits from data research when he or she receives an implantable defibrillator based on a risk prediction model; while the collective privacy of a group would be harmed if this model leads to people with overweight and obesity being excluded from defibrillator treatment for reasons of lifestyle responsibility. Thus, while the debate is often framed in terms of individual versus societal benefits, this distinction is not helpful. Namely, autonomy is a relational property and can be informed by the concept of solidarity.[44,45]

the changes caused by the GDPR. They sometimes fail to see that specific principles and requirements were already included in the earlier Directive. For instance, anonymization requirements have not changed: the new law only clarifies that pseudonymised data is still considered personal data. And with its focus on accountability, the GDPR has brought out certain requirements more clearly. Also, harmonization across the EU may be more effectively pursued if data protection legislation comes in the form of a regulation that applies directly in all countries, in contrast with the former directive. As stated in the law's explanatory recitals, the GDPR was created to establish a higher level of privacy protection within a more harmonised European framework:

> Those developments [technological advances and globalization] require a *strong* and *more coherent* data protection framework in the Union, backed by strong enforcement, given the importance of creating the *trust* that will allow the digital economy to develop across the internal market. (Recital 7 GDPR, emphases added)

This excerpt shows the GDPR's dual aim of a strong and more coherent framework: i.e., better protecting personal data privacy *and* harmonising the legal framework to support data sharing. It also shows that these aims of the new data protection framework require strong enforcement in terms of accountability and transparency, in order to create trust of data subjects (people whose data is used or 'processed') and of data processors and controllers. In what follows, we present a case study of a European research consortium to investigate how these aims of the GDPR play out in practice and what this entails for the privacy-solidarity debate.

11.3 Case study: researchers' experiences with the GDPR

11.3.1 Case study approach and setting

The approach employed in this study is one of empirical ethics, which combines philosophy with ethnographic empirical research.[47,48] In our analysis, we draw mainly on phenomenology to reflect on concepts arising from researchers' experiences.[49,50] The empirical research was conducted using a multiple case study design. Case studies have been described as: an "empirical inquiry that investigates a contemporary phenomenon (i.e., the ethical framework for data protection) within its real-life context (i.e., health research)" (p. 13).[51]

Our case is an international research consortium called ESCAPE-NET (the European Sudden Cardiac Arrest network towards Prevention, Education, New Effective Treatment). This EU Horizon-2020 funded research consortium is building a large database of sudden cardiac arrest (SCA) patients for observational studies aimed

at improving SCA prevention and treatment.[52] Approximately one-fifth of all deaths in Europe are caused by SCA, a condition which is lethal within minutes if left untreated, and survival rates vary between 5 and 20 percent.[53] Because a combination of multiple factors can cause SCA and treatments differ between European geographies, large datasets and international collaboration are needed. Individual datasets may include clinical information collected from hospitals, emergency medical services (EMS), general practitioners and patient surveys, as well as pharmacological, socio-economic and genetic information. ESCAPE-NET combines data from SCA cohorts (~85,000 people), genetic studies (~15,000 samples) and prospective population cohorts (~55,000 people) into one harmonised database with joint controllers.

For the purpose of our case study, a total of ten research groups that contribute patient cohort data to ESCAPE-NET were selected from six European countries (NL, IT, FR, DK, SE, CZ), following guidance recommending inclusion of between four and ten cases.[52] In selecting cases, we ensured that various regions of Europe were represented and different types of cohort studies were included (e.g., those with or without DNA collection). Sources of data included qualitative semi-structured interviews that were supplemented with on-site observations.[55] Moreover, the authors participated in consortium meetings and expert conferences and were involved in the ethico-legal approval processes for ESCAPE-NET. Interviews were conducted with 16 ESCAPE-NET researchers between May and September 2018, around the time of introduction of the GDPR, while observations were done over a three-year period. Interviews were audio recorded and transcribed following written consent, after which they were analysed thematically. We also draw from experience based on interviews about the ESCAPE-NET project with patients and ethico-legal experts.

Of note is that findings relating to the specific protection of SCA data (e.g., on informed consent in emergency settings) will be described elsewhere. Also, we will not discuss scientific governance issues such as practical challenges around data harmonisation. Below, we focus on the experiences of researchers in an international consortium with the ethico-legal governance of observational studies with patient data (our 'case study'). We discuss whether these experiences correspond or conflict with the aims of the GDPR as described previously: a higher level of data protection within the EU, which is harmonized so as to not disproportionally hamper large-scale data processing; and backed by the strong enforcement necessary to create trust.

11.3.2 Data protection without reflection

The first aim of the GDPR is to better protect personal data in an increasingly digital and globalised society. During the GDPR implementation phase, the ESCAPE-NET project's focus was on obtaining approvals from Research Ethics Committee or Institutional Review Boards (RECs/IRBs), devising data processing and transfer contracts, and sorting out legal questions such as in which country to host the server for

the database. Addressing legal challenges was found costly in terms of time, money and workload. In eight of the ten research groups, the introduction of the GDPR hampered research.[v] This burden seemed to decrease when institutions created or updated standard templates (e.g., for data transfer agreements and DPIAs) and as legal advisers became more familiar with the new European GDPR framework. Some costs for the researcher inevitably will remain but arguably this is acceptable given the importance of protecting patients' fundamental data protection rights.

However, while interviewed researchers agreed in theory with the stronger protections afforded by the GDPR, they felt that data protection increasingly comes down to "checking boxes" and using the correct phrasing. Indeed, studies have shown that the effectiveness of DPIAs "varies depending on whether there is in-house privacy expertise [and that] more often than not, they are compliance checks completed without a broader analysis of privacy risks".[56] Before the law came into force, one ESCAPE-NET investigator said he thought that registry research would become easier because the general public would be made more aware of researchers' responsibilities for proper data protection. However, the stronger requirements may not provide practical tools for data protection nor support reflection on underlying values. One researcher expressed his frustration as follows:

> Principal investigator: "This is eating up so much of people's time, and I am really bothered about this, because we spend less and less time on research and more and more time on *doing the right wordings in the approvals*. And if the EU or the government really wants us to continue to do research on such high level, they should really think about how to make it easy and not to... I mean now it is almost like they are not our friends."

When data governance is framed merely in terms of compliance with legal and ethical requirements, a risk of *routinisation* ensues. Ploug & Holm introduced this concept to describe the phenomenon where research participants are asked repeatedly for informed consent, and as a result providing consent becomes an act of routine without reflection.[57] Informed consent then loses its function of protecting autonomy. Similarly, we note that the focus on safeguards and checklists can also cause routinisation among *researchers* trying to practice good data governance. One might argue in an Aristotelian manner that routinisation could stimulate good governance: namely, by cultivating virtue through creating habit and practice among researchers following the data protection procedures.[58] This may be true in simple situations but for more

[v] Partly, this may be due to the fact that with GDPR implementation, data protection fines became higher and oversight stricter – requiring institutions who had not been compliant with the former Directive to bring their outdated data protection policies up to date quickly. The implementation period also made clear the advantages of having a large EU-funded consortium: smaller parties may not be able to bear the data protection costs.

complex research projects working with sensitive health data, we should be aware that stimulating checkbox routine without further reflection can frustrate the underlying moral values of data protection safeguards such as DPIAs.

11.3.3 Incoherent guidance due to disagreement about ethical values

While the second aim of the GDPR is to improve coherence, it still allows Member States their own interpretation of certain provisions including research exemptions.[59] This complicates the establishment of a joint database with different countries.[60,61] For instance, the use of deceased persons' data is not covered by the GDPR but can be regulated nationally[62]: in ESCAPE-NET, some groups could not use these data, which negatively effects study validity and may result in bias. Researchers also noted that their collaboration was affected by national *and* local variation among data protection officers (DPOs) and research ethics committees (RECs/IRBs).[63,64] As a result of different interpretations by experts at participating institutions, a number of studies were stopped until legal questions were sorted out: this took up to two years for some groups.[vi]

Differences in (interpretation of) regulation are due in part to cultural and political factors. For instance, in Scandinavian countries the importance of registry-based epidemiology is engrained in the national culture.[65] Another reason for variation is that laws are necessarily formulated in broad terms and may not apply directly to the specific context, in this case emergency medicine where prospective patient consent is impossible. As Kafka wrote, "it is an extremely painful thing to be ruled by laws that oneself does not know" (p. 128).[66] One researcher summarised:

> Postdoctoral researcher: "There are codes of conduct on using patient material. But they never treat my situation. They do not deal with the issues that I am facing. We have an approval now from the ethics committee, but you still have to go to the DPO and she can still say: no, this is not right."

Several interviewees therefore expressed a desire for more legal guidance. A researcher present at a conference about ESCAPE-NET noted that uncertainty of researchers themselves also harms research:

[vi] For instance, one group created 18 different types of informed consent letters for different types of patients (children, parents of deceased children, adults, legal representatives, et cetera) and based on the kinds of data collected (with or without DNA collection). These letters were revised dozens of times in response to comments by partners who contributed data (ambulance services, hospitals), the legal department, local REC, and DPOs. Only after two years of revisions to these letters, and to the DPIA and study protocol, the study received ethics approval. In addition, as research in emergency medicine is dependent on other partners in the 'chain of care', a data breach at one of the ambulance services temporarily halted the supply of data from that data source.

> Researcher: "The ethics committee and data protection officers told us: the law does not keep you from doing your research. It is only your own fear and uncertainty of doing the research and taking the risk of data breaches if you don't know what you are doing."

However, all laws remain to a certain extent open for interpretation. A legal expert with whom we spoke about ESCAPE-NET commented on why there is so much discussion among jurists: "one might lean more towards the principle of privacy protection, whereas another might attach more value to scientific research and data sharing". Law can be seen partly as solidified morality, so the underlying issue is one of ethics, and the different interpretations can be traced back to the privacy-solidarity debate discussed earlier. Van Veen rightly noted that "[legal texts] could be subsumed under informational self-determination versus solidarity" and "the future of biomedical research in Europe will be decided not only by the GDPR text but also by the outcomes of the debate on those values".[59]

We already noted in the background section how privacy and solidarity are difficult to define. Moreover, there is no objective evaluative standard for balancing these values. An appropriate shared standard may be especially difficult to find in international collaborations if partners do not share the same morality.[67] What can be considered good governance, depends on contextual factors and there is no one fundamental value to ground our actions. Philosophers have long known that all rules may ground out on something arbitrary and merely stem from how we choose to organise society. As Kant said, metaphysics is an ocean without shore and lighthouse (2:66.1–6).[68] In this ocean of uncertainty, our values are like planks of a floating raft that can only be built into a ship by standing on one of the other planks – one cannot stand outside the raft or find final principles by diving down[69,70]; or like a wiki where all entries link to each other based on how the developers decide they should.[71] Therefore, both privacy and solidarity are in a sense 'without ground' and finding a good balance between them requires *trust* as the rope that keeps the raft together: as the basis for the social contract between researchers and data subjects.

11.3.4 Strong regulation may crowd out trust

We noted how the GDPR text mentions strong enforcement of the regulation as a condition for creating trust. Between ESCAPE-NET researchers, the level of pre-existing ('ontic') trust was high. For instance, when discussing whether oversight on the scientific quality of studies was needed, one of the executive committee members did not find this necessary because "they know what research is and I trust their judgement". Trust makes cooperation easier as it removes incentives for monitoring.[72] Researchers who trust each other to handle data responsibly, and who enjoy

collaborating, are more likely to share data.[13] Indeed, in ESCAPE-NET trust between scientific partners leads to solidarity in data sharing and collaborating for patients' benefit:

> Principal investigator: "It's a good group as well. You know, when you do research it's a lot about trust and that's something I think we have in this group. We know each other from previously. We know of each other's work. I mean it is a question of whether they use the data correctly. Ethical and trust is a bit the same in these situations. That they use the data correctly is one thing, and of course the breach of data... If they are not secure enough. And that is difficult when you are not there, so you really need good trust."

However, the complexity of data protection requirements and data sharing contracts, combined with the risk of high fines, undermined collaboration between researchers: regulation may thus 'crowd out' trust. The *crowding-out effect* is a term from economics to describes cases where over-active governments supplant citizens and businesses in the market. In our case study, we saw that strict legal measures (related to the GDPR or to requirements for medical secrecy) led to researchers having difficulty in cooperating with external data suppliers like hospitals or ambulance services who became hesitant to share, or with RECs and DPOs who became increasingly cautious in approving research proposals. ESCAPE-NET is a relatively young project that mostly shares data within the consortium, but the legal complexities may complicate future cross-consortium collaborations, as was seen in other studies.[13] On the other hand, legal contracts may play an important role in promoting trust between these parties by demonstrating reliability and reducing uncertainty, especially when societal values are in flux. They serve as an implementation of the social contract and as what Hannah Arendt called islands of predictability: "to make a promise is to predict the future".[73]

A similarly complex association between regulation and trust is seen for the relationship with data subjects. Trust has always been characteristic for the physician-patient relation where patients enter the "sick role" exempting doctors from ordinary people's responsibilities, and a key function of medical research ethics codes is to foster public trust.[74] We trust doctors partly because we know they are covered by contracts, professional codes, and laws. However, public trust in science has been declining in the past decades, and a lack of trust reduces research participation and negatively impacts the public's perception of research.[75; vii] In a study from the United States, patients' trust in researchers was the most powerful determinant for the kind

[vii] For ESCAPE-NET, this was experienced in a minority of studied research groups that reported declining consent rates after May 2018, but we do not possess quantitative data about the effects of media-attention surrounding the GDPR on patient participation.

of control they desired over their medical records: when trust is low, patients desire explicit informed consent.[76; viii] Thus, the response to worries about trust often consists of increased regulation and oversight, including requirements of accountability and transparency, and the creation of contracts such as informed consent forms and data sharing agreements.[79,80] Wolpe has referred to these as 'rituals of trust'[17] that emerge when ontic trust is scarce, and the stronger enforcement promised by the GDPR may be an example of such a ritual of trust.

In summary, trust in health data research is not incompatible with regulation, but after a certain threshold the gathering of information to ensure that the other party can be trusted, will destabilize the pre-existing relation of trust.[81,82] After this threshold, rituals of trust can create distrust that complicates cooperation and data sharing for the public good.[ix] As such, a paradox arises where *"the commonality of rules, which can only exist if there is unconditional trust, becomes itself a precondition for trust and hence a source of mistrust"* (p. 94).[84] This circular relation between trust and regulation thus requires delicate balancing.

11.4 Towards trust-based governance of health data research

We have seen that the aims of the GDPR were not reflected in researchers' experiences in our case study. The current data protection framework can have the potential negative effects of reducing data protection to checkbox exercises, leading to incoherent guidance, and crowding-out of trust. Given the uncertainties and contextual factors at play in health data research, neither privacy nor solidarity can serve as the sole foundational value. In an article about technologically mediated homecare, Kamphof frames privacy "as a gift of trust" to health care professionals[23]; in another paper by Allen et al. the social license for health research is said to be grounded in trust.[85] Indeed, what is needed is not a search for final principles but a re-appreciation of trust. To support this, in what follows we propose a three-part framework for trust in health data research: establishing trust as a multi-agent concept; that is rational and democratic; and that can help with priority-setting among ethical values.

[viii] Of note is that also the response at the other end of the spectrum, i.e., enforcing solidarity rather than privacy, will cause trust in health data research to wither.[77,78] Solidarity understood as a means to keep society together ('solid') cannot be required from the top down, but can stem only from shared trust.

[ix] Distrust, which serves to protect from tyranny or oppression, has received little attention in the philosophical literature, possibly because it is considered less risky than misplaced trust.[83] However, the harm of distrust may lie in the non-use of data which does have important societal consequences.

11.4.1 Trust as multi-agent concept

Trust is needed in the world as it would not be economically efficient, nor practically possible, to have everyone know and control everything that affects them (e.g. scientific knowledge is impossible without trust: we have to trust scientists' testimony in believing that the earth is round). In the previous section we saw that the commonality of rules is based on unconditional trust. Thus, trust is a type of social capital that enables people to cooperate.[86] William James, an early phenomenological philosopher,[87] noted that ethics by definition involves trust in others: we cannot always wait for evidence as we might risk missing out on valuable societal truth.[88]

> *A social organism of any sort whatever, large or small, is what it is because each member proceeds to his own duty with a trust that the other members will simultaneously do theirs. Wherever a desired result is achieved by the cooperation of many independent persons, its existence as a fact is a pure consequence of the precursive faith in one another of those immediately concerned.* (Section IX)

The dominant philosophical paradigm of trust is one of interpersonal trust, e.g. between doctor and patient, and trust has been defined simply as *the belief that the trustee will put the truster's best interests first*.[89] However, this common conception of trust does not suffice for our case. Complex health data research is better compared to a multi-agent system (MAS) in computer science. Similar to a MAS, health data research is composed of multiple interacting intelligent agents and their environment, that must act together to solve complex problems. In our case study, we encountered many mentions of trust at different levels, between various people and organisations. This reflects what David Resnik calls a "web of trust" where trust connects all actors in the medical research enterprise (i.e. the people building the raft or wiki together), including research sponsors.[90]

For instance, recall how one of the ESCAPE-NET investigators said about the European Commission that it was "almost like they were not *friends* anymore", which shows betrayed trust rather than misplaced reliance.[x] The relation with RECs/IRBs is similarly one of trust, as investigators need to be able to trust that their studies are reviewed fairly and competently (which is sometimes problematic when REC/IRB members do not have expertise in big data)[93].

---

[x] Trust is not mere reliance,[91] but reliance "plus some extra factor".[92] In an exploration of trust in the context of the UK's National Health Service, Sheehan et al. showed that this extra factor lies in the fact that trust is associated with gratitude when vindicated and with betrayal when it is not.[79] According to Baier, betrayal is the appropriate response when someone is relied on to act out of goodwill.[81]

As we saw in our case study, researchers must also be able to trust *each other* to behave competently, ethically, and professionally.[94] In addition, artificial agents can also be trusted or distrusted, which was not apparent in our case study but is a point to consider when artificial intelligence and robotics become more prevalent in the healthcare setting.[95]

Trust is also important in the relationship between participants and researchers. In our case study, researchers believed data breaches would be harmful as they lead to a breach of trust in the research enterprise. For clinical research, trust is often quoted as people's reason for participation.[96] Similarly, several ESCAPE-NET researchers thought that "the trust in the researcher should be enough" for people to decide to contribute data. In a study where we interviewed SCA patients who contributed to ESCAPE-NET, we found that trust was indeed one of the key factors for people when deciding to share their personal data for research.[97] This trust mainly stemmed from their positive experiences with clinicians and with the medical institution conducting the research. Brown analysed trust among gynae-oncology patients using the work of the phenomenological philosopher Alfred Schütz and found that patients, in seeking to trust, explained away any media-related fears.[98] In Brown's and our studies, this type of confirmation bias seemed to come from a 'will to trust', e.g. a will to contribute to health research in order to help future others.

Of note is that big data is mediating the relation between patients and researchers in a new way, with the ethical duties less visible due to the distant and sometimes anonymous nature of the relationship. Moreover, health data research is increasingly performed by non-clinicians like experts in machine learning or epidemiology, and generalised trust in doctors does not suffice anymore. These factors complicate the creation of trust and seem to reduce the public's will to trust researchers. If trust becomes increasingly scarce, this negatively impacts study recruitment as we saw in our and other studies.[99] So when aiming to promote trust in big data studies, it is important to take into account the more distant relation with researchers, and to focus not only on data subjects but on all actors in this multi-agent system.

11.4.2 Trust as rational and democratic

The only protection from the unknowable is the suspending of judgment (a Husserlian 'bracketing' of the world, if you will), but this act of trusting involves risk and constitutes at first sight an inherently irrational decision.[100] Acts of trust may be *prima facie* irrational actions, but can in fact be highly rational, says Brown in reflecting on Kierkegaard's idea of the 'leap of faith'.[98] Professionals who are friendlier or more patient are likely to deliver more positive outcomes: thus emotions of trust can constitute a rational response to unconscious ideas about correlations between the communicative signs and the motives of the trustee. Rationality is often mistakenly equated with certainty. By drawing on previous lived experiences, data subjects will

not have definite predictions of the future but can know (*feel*) how to act in uncertain circumstances. And even in absence of previous experience, trusting may still be rational when aiming to minimise anxiety about uncertainty in situations of vulnerability (e.g., when assuming the aforementioned sick role in relation to healthcare professionals; and perhaps especially in relation to emergency care providers)[101]. Health care and research function in a system of societal norms, with its contracts and safeguards, and thus make trust plausible for socially embedded agents.[102]

To ensure that this trust is not misplaced, however, researchers should give *reasons* that serve as *trust-tags* within a particular environment or context (p. 40).[71; xi] After all, it is the human capacity for reasoning together that makes moral progress possible.[105] Neither privacy or solidarity is more rational than the other, but discussion about these principles leads to *more democratic* decision-making about health data research. French philosopher Emmanuel Levinas argued against Heidegger that ethics does not have an essence but occurs out of concern for the Other: across the hiatus of dialogue instead of in the content of discourse ("the said does not count as much as the saying itself" (p. 42)).[106] Therefore, in order to engage in deliberation, those involved need to accept that actions are essentially unfounded but that they still stand on a shared societal normative framework. In practice this means that rather than asking people to have blind faith, health data researchers can create trust-tags by publicly explaining their policies and by providing patients and other researchers with information about data uses and oversight mechanisms.

Because data collection is always embedded within a particular culture and trust is different in different social contexts,[107] it has been suggested that 'ethical metadata' may be useful to promote trust in international studies: i.e. the addition of information to datasets about the normative context of the study, such as the consent conditions that need to be respected when data is shared with other researchers.[108,109] Another way to promote trust is via public and patient engagement (PPE) during the planning and implementation of studies, for instance through a steering board with patient representatives.[110; xii] In their communication efforts, researchers need not

[xi] Whether one ought to trust or not, is relative to contextual factors.[103] Similarly, the right to data protection is not absolute but context-dependent, as it "must be considered in relation to its function in society and be balanced against other fundamental rights" (GDPR Recital 4). For example, it is conceivable to tend towards solidarity for public health research and towards privacy for certain commercial uses. This balancing act is influenced by public opinion and depends on how the GDPR is interpreted by experts, policy-makers, oversight bodies and courts: "the life of the law is the plaintiff".[104]

[xii] In ESCAPE-NET, most groups disseminated findings but did not involve patients in the design of the research. Some researchers thought PPE would be especially valuable in emergency medicine given data subjects' greater vulnerability, and believed that PPE would improve study quality and relevance. Others did not see the need, given the lower risks associated with observational studies compared to clinical trials, or expressed concerns about the representativeness and knowledge of patient panels.

fear being transparent about risks and uncertainties, as communicating uncertainty only has a minor impact on people's trust.[111] Especially engagement with people who distrust researchers, can be an opportunity to make policies more trust-promoting. While researchers should be trustworthy, the research subject as truster also has a responsibility, namely to be understanding and receptive to trust-tags.[xiii] It is impossible to require guarantees against all harm and "the existence of the abyss is beyond the patient's control, but they have materials for bridging the depth of uncertainty".[98] The truster must be content with some level of vulnerability, as we saw that an overemphasis on monitoring will crowd out trust.

11.4.3 Trust as method for priority-setting

If after the exchange of reasons, moral conflicts remain between key principles of biomedical ethics (autonomy, non-maleficence, beneficence and justice), trust is useful for *priority-setting*. This idea has been elaborated by Resnik who argues that in clinical research a fifth principle ('promote trust in research involving human subjects') can help investigators and oversight bodies to set priorities and to resolve disputes involving the interpretation of regulations (p. 105).[90] In case of conflict, researchers ought to ask themselves how one action or another would impact on people's trust (of note is that promoting trust is not a 'meta-rule' but a prima facie rule that may conflict with other principles as well). In our view, the fifth principle also applies to non-interventional health research with data and helps deal with the moral dilemmas (e.g. privacy vs solidarity) inherent to data sharing.

For instance, in the case of ESCAPE-NET, the consortium leaders are facing the challenge of sustaining the database after project funding ends, and are deliberating whether attracting commercial funding would be an option. In their deliberations, they could use the principle of trust as an additional aid and apply the moral test of trust, asking: 'Would patients' trust be damaged if they found out about this practice?'.[81] If the initiators of the failed *care.data* programme in the UK had used this principle, they might have chosen better trust-promoting ways of informing the public about (commercial) data uses and may have still been operative.[113] Even for minimal-risk observational studies, asking consent from data subjects may be valuable to create trust, as it shows that researchers are transparent and that they take patients' preferences seriously. In order to facilitate the data subject in perceiving the researcher as competent and caring, incorporating trust into decision-making thus requires good communication.[114]

[xiii] Trustworthiness differs from trust in that it depends on features of the trustee, as a type of moral virtue or property,[112] while the act of trusting is an attitude that depends on features of the truster.

11.5 Concluding remarks

In our case study of the ESCAPE-NET consortium, we found that while the central aims of the GDPR are compatible with stimulating health data research, the implementation in practice can be problematic. Formalised measures like extensive DPIAs can lead to routinisation among researchers, which may cause data protection instruments to lose their protective function, although quantitative study on the effect of routinisation is needed. In addition, the lack of (inter-)national coherence in legal requirements and in interpretations by DPOs and RECs undermines the harmonization function of the GDPR and complicates data sharing.[115] The different legal interpretations stem partly from different views on the right balance between privacy and solidarity. Our empirical-philosophical method brings a new perspective to this debate, as it suggests that the key does not lie in recognising either privacy or solidarity as foundational, but in a re-appreciation of trust as basis for science's social contract. The case study shows that enforcement of privacy measures may build trust, but that overly restrictive measures destabilize the trust relation between different actors. We provided a three-part conceptualisation of trust that may help to promote responsible governance of health data research: trust as multi-agent concept; as rational and democratic; and as a method for priority-setting.

This case study may not be generalizable as we looked at a European consortium where pre-existing trust was high. In contrast, in collaborations of researchers from high income countries with researchers from low and middle income countries, trust may not be sufficient given existing power asymmetries.[116] Similarly, in research with people from underprivileged communities, a model of participant-researcher relations based primarily on trust might reproduce power and knowledge asymmetries, and alternative models should be sought.[117] Additional study is also needed on the conditions for conducting health data research in partnership with commercial companies which may reduce public trust.[118] For instance, commercial access could be limited to uses that promote the public interest.[21]

We believe that the creation of practical guidelines for creating trust between the different agents in the research system requires dialogue with these stakeholders, which may be done through PPE or interdisciplinary expert groups.[23] Efforts are needed to make those initiatives inclusive and representative, and further study should explore how to support the public in being responsible trusters. For instance, insights may be obtained from research with tissue samples or from non-medical contexts, to transpose solutions that worked in those settings.[119] In addition, ethics education for data researchers could support them in relating data protection rules to wider values and norms (such as human rights) as a reminder of the societal fundament of rules, which may help prevent harmful effects of routinisation. We also note that specific ethical and legal support is needed for researchers to empower

them in safeguarding participants' rights, to ensure that people's trust is well-placed. Guidance may take the shape of codes of conduct or expert advice, which calls for increased collaboration between RECs, DPOs, ICT security and legal experts.

The promotion of trust also requires recognising the limitations of localized oversight in an ICT-based research world, since health data research does not follow the traditional model of "one subject, one researcher, one jurisdiction".[109] Increased harmonization of data protection guidelines and ethical approval processes for observational studies can help to protect patients' rights and to promote collaboration for creating larger and more valid datasets.[64,120] In order to avoid replication of review, the ethics review of observational research could be modeled after efforts to harmonise clinical trial review processes.[121] Harmonization requires, however, international agreement on definitions of bioethical concepts such as solidarity, as well as on data protection terminology such as what constitutes anonymous data.[15,122] Innovative policy solutions, like the use of ethical meta-data when sharing datasets, are needed to ensure that the governance of international collaborations is based on the values of involved patients and researchers.[108,123]

Finally, we wish to stress that initiatives aimed at building trust should not be one-time affairs but require responsiveness to changes as "our dynamic society requires a dynamic morality".[124] One area where views seem to be changing is the use of deceased persons' data for research which has been largely unregulated at international level, and it is important to investigate the moral basis and implications before any practice becomes socially embedded. Moral change around concepts like privacy and solidarity is induced by big data analytics, and normative frameworks may continue to be adapted with the growing use of artificial intelligence and machine learning methods in health care and research. Where these methods run into problems around the explainability of algorithmic decision-making, trust will become vital.