

Governing Health Data Across Changing Contexts: A Focus Group Study of Citizen's Views in England, Iceland, and Sweden

N. Shah¹, J. Viberg-Johannsson², E. Haraldsdóttir³, H.B. Bentzen⁴, S. Coy¹, D. Mascalzoni^{2,6}, G.A. Jónsdóttir³, J. Kaye^{1, 5}

¹ Centre for Health, Law and Emerging Technologies, Faculty of Law, University of Oxford, Oxford, UK

² Centre for Research Ethics & Bioethics, Department of Public Health and Caring Sciences, Uppsala University, Uppsala, Sweden

³ Social Science Research Institute, University of Iceland, Reykjavik, Iceland

⁴ Norwegian Research Center for Computers and Law, Faculty of Law, University of Oslo, Oslo, Norway

⁵ Centre for Health, Law and Emerging Technologies, Melbourne Law School, University of Melbourne, Australia

⁶ Institute for Biomedicine, EURAC Research, Bolzano, Italy

Corresponding author

Nisha Shah, Centre for Health, Law, and Emerging Technologies (HeLEX), Faculty of Law, University of Oxford, Ewert House, Ewert Place, Summertown, Oxford OX2 7DD

Email: nisha.shah@law.ox.ac.uk

Keywords

Health data, data sharing, data governance, public trust, data privacy, public attitudes

Abstract

Introduction: The governance structures associated with health data are evolving in response to advances in digital technologies that enable new ways of capturing, using, and sharing different types of data. Increasingly, health data moves between different contexts such as from healthcare to research, or to commerce and marketing. Crossing these contextual boundaries has the potential to violate societal expectations about the appropriate use of health data and diminish public trust. Understanding citizens' views on the acceptability of and preferences for data use in different contexts is essential for developing information governance policies in these new contexts.

Methods: Focus group design presenting data sharing scenarios in England, Iceland, and Sweden.

Results: Seventy-one participants were recruited. Participants supported the need for data to help understand the observable world, improve medical research, the quality of public services, and to benefit society. However, participants consistently identified the lack of information, transparency and control as barriers to trusting organisations to use data in a way that they considered appropriate. There was considerable support for fair and transparent data sharing practices where all parties benefitted.

Conclusion: Data governance policy should involve all stakeholders' perspectives on an ongoing basis, to inform and implement changes to health data sharing practices that accord with stakeholder views. The Findings showed that 1) data should be used for ethical purposes even when there was commercial interest; 2) data subjects and/or public institutions that provide and share data should also receive benefits from the sharing of data; 3) third parties use of data requires greater transparency and accountability than currently exists, 4) there should be greater information provided to empower data subjects.

Background

Digital technologies are becoming the backbone for a data-driven health sector (1, 2) helping to integrate electronic health records, smartphones and applications, biosensors and 'omics' (3) data. Research data, routinely collected data from within and outside of healthcare, and large aggregated national and international clinical research datasets, are anticipated to be more widely used to understand and address healthcare issues and make evidence-based healthcare decisions (4-6), as advocated by the EU Open Science agenda (7). Moreover, the possibility to link patient data to commercial data such as insurance, purchasing habits, and travel itineraries may provide more nuanced understandings of individual health, behaviours, and lifestyle (8, 9) however, critical issues remain about using health data for secondary purposes. These centre on privacy and the security of data, who can use the data, for what purposes, and who will benefit from its use.

Public concerns about privacy in the biomedical research and healthcare delivery context have been well documented (4, 10, 11) , however, health data also proliferates in other contexts (12, 13). For instance, health and wellness mobile apps, may collect health data that is routinely shared with third parties (14-17). The user-generated lifestyle data from these apps can also be useful for healthcare providers to monitor and treat illness (17, 18). Public confidence in health data sharing has been affected by recent data breaches in Europe. In Sweden, 2.7 million recorded patients' phone calls with a healthcare contractor were downloadable via an unprotected web server (19). In Denmark, a local health authority database maintained by a private company was ruled to have illegally collected patient data, as it collected more data than it was permitted (20). Many digital platforms fail to ensure users' privacy due to the lack of transparency about their data sharing practices (14, 21, 22). Privacy policies often lack information about what data may be collected from data subjects, for what purposes and with whom it may be shared, and are sometimes not available at all (23). Some public-private partnerships have also received scrutiny as data sharing agreements do not align with data subjects' reasonable expectations (e.g., DeepMind and NHS case) (24, 25).

While transparency is a key attribute of data governance, the trade-offs citizens are willing to make regarding the secondary uses of their data depends on several factors. Public acceptability of the use of health data varies, depending on individual awareness, interest, socio-demographic characteristics, and cultural norms (individualistic vs collectivist norms) (5, 26, 27, 28, 29). Beyond this, acceptability depends on the contextual cues where data types have different meanings and are applied and understood differently in different settings. For some individuals, use of health data outside of healthcare may be acceptable, and for others it may not (30-32, 33, 34).

To date, research has mostly focused on patient or research participants' views about sharing data for biomedical research or healthcare planning (35-37), and prioritised attention to informed consent (5, 10, 38, 39). The current study explored further on citizen perspectives about the purposes for sharing health data where it proliferates, as the users may encompass companies and non-medical experts, and purposes may include marketing and advertising, and product development as well as biomedical research and improving healthcare delivery.

Using Nissenbaum's theory of contextual integrity (CI) (30-32), which explains that privacy is perceived and expected differently depending on the norms and values surrounding the context, the study sought participants' reasonable expectations for when health data is shared for secondary purposes in broader contexts.

According to Nissenbaum (30-32), when data moves to a context with different norms and values, this is a breach of contextual integrity. Integrity depends on: involved entities (sender, receiver), purposes, and transmission principles (conditions by which information may flow). Previous research has found some support amongst the public for the sharing and secondary uses of patient data for research, and planning and delivery of healthcare (35-37). While trust in healthcare institutions for handling data is highest for these purposes, it varies considerably between entities situated in different contexts (40, 41). The highest trust is given to primary

care-providers and the lowest to commercial and media companies (40, 41). It is often the commercialisation of data that concerns people in Europe, and as a result commentators have suggested that governments need to develop governance and policies to balance the rights to privacy and confidentiality with the use of data for different types of purposes (6).

Public deliberation and a continued dialogue on factors affecting acceptability of health data flows between and within contexts as well as preferences for governance is essential to address the 'data trust deficit' in internet companies that use personal data (42). Public attitudes are influenced by the level of awareness and understanding of how health data may be used and handled within the context of personal and collective benefits (5, 26, 29, 43). There has been public deliberation research about the acceptability of data sharing and reuse and mechanisms by which these should be governed (4, 8, 44). However, to date, understanding and establishing appropriate governance strategies for health data sharing have mostly focused on reuse of data for direct health care, research purposes, and attitudinal research confined to informed consent processes (5, 10, 38, 39).

Given the complexity of digital health data flows and the increased likelihood of public-commercial linking of data, public concerns persist. Understanding public knowledge of data flows for purposes other than direct healthcare and related social values are integral to explaining why social norms may be breached in novel health data sharing contexts and what members of the public would like governance of health data to achieve. This was the focus of the current study which engaged people in England, Iceland, and Sweden. These countries were chosen because of the similarities in breaches of trust among the public regarding secondary uses of health data such as the Care.data initiative in the UK, Sweden's Medical data breach, and the population database proposal in Iceland by the company deCODE to name a few. While between-country differences exist, this study sought to identify similarities in public perspectives about health data flows and governance applications.

We aimed to define the factors involved in participants' deliberations about their expectations of data flows and governance of secondary uses of health data relating to contextual cues: a) To understand factors affecting public perceptions and acceptability of health data sharing when contextual integrity is breached and values associated with trade-offs; b) To characterise participants' experiences with their health-related data being shared in different contexts; and c) To identify preferences for health data governance for data flows in different contexts.

Methods

Study design

This was a semi-structured and scenario-based focus group study. The scenario approach enabled discussions of ideas and preferences for the governance of health data in the context of realistic flows of health data. This was due to the expectation that lay people are concerned individuals who have valid opinions about how data should be governed but may have differing levels of awareness and interest in how data sharing occurs and how it should be governed.

Recruitment

Participants were recruited during June – October 2019 in England, Sweden, and Iceland at major cities and where possible in rural locations. Participants had to be at least 18 years of age. In England, participants were recruited using convenience and snowball sampling, through advertising in community centres, libraries, local information websites and news publications. The English participants that contacted the research team were sent the study information sheet and consent form and invited to attend the focus groups scheduled to take place nearest to their locality. In Sweden and Iceland, participants were contacted by telephone and recruited through lists of randomly sampled individuals drawn from their respective national registers and invited to participate in the focus groups after receiving the study materials by post or email. These lists were representative of the populations by age, gender, and educational attainment. The recruitment was stopped once we had achieved saturation, meaning no new viewpoints were identified after 10 focus groups combined.

A total of 13 focus groups were conducted across the three countries (Table 1). A socio-demographic questionnaire including questions relating to the use of the internet and mobile technologies was disseminated to the attending participants (Appendix A). The focus groups lasted between 90 and 135 minutes overall and were audio recorded and transcribed verbatim into each language.

Discussion guide and scenarios

A discussion guide and script were developed to include three components: 1) A warm-up section asking about participants' experiences with using the internet and social media, and digital technologies such as smartphones and mobile applications; 2) Introduction of data governance concepts, and 3) A scenario-based narrative following a hypothetical individual illustrating how health data may flow from one context to another (Appendix B). The components aimed to elicit participants' experiences, concerns and governance expectations about the way health data could be captured, used and shared digitally, including healthcare records, mHealth apps and wearables.

The scenarios were informed by information-gathering discussions with stakeholders (legal experts, policy think tanks, and academics), and a rapid literature review of data sharing research and prominent data sharing cases in each country for e.g. DeepMind and Royal Free case in the UK (25). The topics for inclusion were extensively discussed by the research team to ensure the data gathered would be comparable across the countries studied. The content was organised using contextual-integrity heuristic (30-32) and described normative health data acquisition such as data typically collected and shared through direct healthcare, mHealth applications and wearable devices, the purposes of using the data, and the sharing and use practices of different actors (clinicians, scientists, local and national government, and technology, pharmaceutical and other commercial companies). The scenarios prompted how

participants made sense of the uses of data and if trade-offs were made, what these would be influenced by.

The discussion guide was developed in English and translated into Swedish and Icelandic. It was then piloted in small groups of lay people in UK, Sweden and Iceland, and content and language checked for meaning by the local research teams (NS, JVJ, EH and GAJ) to ensure the translations were accurate. Revisions to the guide and scenarios were also based on the suggestions of the pilot participants.

Analysis

Data analysis followed the Framework Analysis approach (45, 46), where the initial framework was developed by review of two transcripts and applied to subsequent transcripts. To allow ongoing inclusion and refinement of emergent codes, the framework was both deductive and inductive. Three Researchers (NS, JVJ, EH), supported by the wider team, convened regularly for analysis to ensure shared understanding and coding consistency of transcripts. The emerging themes and interpretation of the data were discussed in a final 3-day workshop. The results and quotes are presented here in English (translated from Icelandic and Swedish by the research team) to illustrate points.

Ethical approval

Ethical approval was granted in all three research institutions where the study was conducted, by the University of Oxford Central University Ethics Committee (R63378/RE001), the Swedish Ethical Review Authority (2019-02590) and the proposal reviewed by the University of Iceland Science Ethics Committee (VSH-2019-019).

Results

Participant characteristics

Overall, there were 71 participants in the study: 32 in the UK, 17 in Sweden, and 22 in Iceland. Each focus group had between 4-9 participants. Participant demographics are presented in Table 1. Overall, there were more female participants, the number of participants in each age group was similar across the countries, and a higher proportion of participants in England and Iceland had higher educational attainment compared with Sweden's participants (see Table 1). More than 3 out of 4 participants reported having experience of using digital devices such as a laptop, smartphone, and computer. Approximately 1 in 4 participants had used a smartwatch. Nearly all participants used the internet and mobile apps at least once a day, however, 37% of all participants had not used a mHealth app.

	Sweden (n=17) ^b	England (n=32)	Iceland (n=22)	All (n=71)
Focus groups (n)	2x Uppsala	2x Oxford	2x Reykjavik	13
	2x Sala	2x London	1x Egilsstaðir	
		1 x English village		
		1x Manchester		
Gender				
Male	7 (41.2)	10 (31.3)	9 (40.9)	26 (36.6)
Female	10 (58.8)	22 (68.8)	13 (59.1)	45 (63.4)
Age				
18-30	4 (23.5)	7 (22.6)	3 (13.6)	14 (20)
31-40	3 (17.6)	7 (22.6)	3 (13.6)	13 (18.6)
41-50	2 (11.8)	3 (9.7)	5 (22.7)	10 (14.3)
51-60	1 (5.9)	3 (9.7)	3 (13.6)	7 (10)
61-70	4 (23.5)	9 (29)	4 (18.2)	17 (24.3)
71+	3 (17.6)	2 (6.5)	4 (18.2)	9 (12.9)
Highest level of education				
≤Secondary/high school	11 (64.7)	5 (16.1)	7 (31.8)	23 (32.9)
Vocational/professional	0	4 (12.9)	3 (13.6)	7 (10)
≥Bachelor's degree	6 (35.3)	21 (67.7)	12 (54.5)	39 (55.7)
Other	0	1 (3.2)	0	1 (1.4)
Devices used by country				
Desktop computer	16 (100)	27 (87.1)	19 (86.4)	62 (89.9)
Laptop	15 (93.8)	27 (87.1)	21 (95.5)	63 (91.3)

Smartphone	14 (87.5)	28 (90.3)	19 (86.4)	61 (88.4)
Tablet	13 (81.3)	26 (83.9)	17 (77.3)	56 (81.2)
Smartwatch	3 (18.8)	7 (22.6)	9 (40.9)	19 (27.5)
Frequency of internet use^c				
Once to multiple times a day	16 (100)	28 (90.3)	20 (90.9)	64 (92.8)
Less than once a month to a few dozen times a month	0 (0)	1 (3.2)	0 (0)	1 (1.4)
Seldom or never	0 (0)	2 (6.5)	2 (9.1)	4 (5.8)
Frequency of mobile apps use^d				
Once to multiple times a day	14 (93.3)	27 (90)	18 (85.7)	59 (89.4)
Less than once a month to a few dozen times a month	1 (6.7)	2 (6.7)	1 (4.8)	4 (6.1)
Seldom or never	0 (0)	1 (3.3)	2 (9.5)	3 (4.5)
Use of mHealth apps				
Yes	11 (68.8)	21 (67.7)	10 (50)	42 (62.7)
No	5 (31.3)	10 (32.3)	10 (50)	25 (37.3)

Table 1: Participant demographics and use of digital technologies by country^a

^a Not all participants answered all questions, and percentages are calculated on valid n.

^b n(%)

^{c & d} Collapsed categories for ease of interpretation

Focus group results

The focus groups explored public perceptions of health data flows within and between contexts, to understand the issues that concern participants when data is shared across contextual boundaries. In particular, the focus groups sought to elicit perspectives about digital technologies, the factors affecting perceptions of trust and what is considered acceptable when health data is shared and used for secondary purposes in different contexts. Overall,

participants believed that trust in the entities that handle data hinged on due accountability, the right amount of oversight, and fairness in the distribution of benefits from the use of data. These perspectives culminated in five core themes. The first two themes described participants' digital world views: 1) Awareness of health data crossing contextual boundaries, 2) Moral expectations and obligations for future data sharing. The final three themes defined the factors affecting trust and acceptance of health data sharing between contexts, and these were: 3) Information provision and individual level control, 4) Oversight and accountability of health data re-use, 5) Fairness in data use, representation, and reciprocity.

Digital World Views

An increasing digitalised world has brought new challenges to how privacy is protected and perceived and what is regarded as appropriate standards for the security of personal data in various settings. Laws and regulations are not always in step with the pace of innovation, which often creates uncertainty about how the law may apply and what constitutes ethical practice. This can result in a diversity of approaches and standards across different contexts and new spheres of activity which leads to a perception that technological innovation is challenging existing ways that things are done. This sentiment was articulated across focus groups in all three countries. The themes show how participants described their a) awareness of health data crossing contextual boundaries and b) the moral expectations for future data sharing.

1. Awareness of health data crossing contextual boundaries

The context and purpose for which data may be used was significant in participants' reactions to descriptions of secondary uses of their personal or health data in all countries. For many of the participants the purpose of the use of data was the most prominent issue about data sharing and participants stated that they did not have a problem sharing data if the purpose is good. A good purpose would be defined as data sharing that saved lives or developed a product that made people feel better. However, even if the purpose is good, participants

preferred to know what the data would be used for. Lack of transparency about the purpose of the use or sharing of data was perceived negatively and where users solely benefitted financially from sharing data was not a good enough purpose (Textbox 1).

SWE: “Yes, the purpose is important... a good purpose. But if they [mobile applications] want access to [data]... or check my photos and my contacts in the mobile and so, then I would be sceptical. Because there is no reason for that” (FG3, Uppsala, P17, Female, age (preferred not to say))

Many expressed implicit or explicit trust in the national health services and public health authorities in all countries. Participants expected that patients’ best interests would be a priority and assumed that as the health sector would be heavily regulated, health personnel would be subject to a duty of confidentiality that would apply to the data usage (Textbox 2).

ENG: “I’ll go back to what I said about the NHS, I assume ... there are rules in place that would not allow a GP to give your data away. That must go up to the level where that data is in a bigger... place. I make the assumption its safe.” (FG3, English rural village, P16, Female, aged 61-70)

However, the increasing visibility of private contractors providing infrastructure, support, and services appeared to undermine expectations. This discussion was prominent in the English focus groups (Textbox 3).

ENG: “I think with changes to the NHS that have come in ... you have different contractors that are not NHS come in and your health information has to be shared with them... they don’t have the same intentions. They might sell that information on; and you don’t know who they’re selling that information on to. It could be like completely innocuous but you as a patient, you’re not aware of who that third party is

going to be. Like, it could be a medical device company, fine, but that medical device company is going to make profit from my data ... and I unwillingly have participated in providing profits for this medical device company that might not be needed in lots of cases.” (FG5, London, P22, Female, aged 31-40)

The intentions of private organisations wanting to use patient data extracted from the healthcare system were a concern. A recurring assumption was that data would be linked for marketing and advertising (Textbox 4).

SWE: “If we take diabetes for example, then [data of] everyone who has diabetes going through the hospital... ends up in companies and then bombs them [patients] with advertising” (FG3, Uppsala, P15, Male, aged 71+)

2. Moral expectations and obligations for future data sharing

In all countries, the participants expressed that there was great value in the use of health data. In Iceland, some participants argued that if their medical data would be used for research and improving population health, then there was a moral duty to allow that data to be reused. This potentially stemmed from public debate about health data linkage from health records to understand population health. Similarly, in the English and Swedish samples, research purpose was a highly acceptable situation for the re-use of data, though participants felt that restrictions should be in place when private companies wanted to access data. There was support for health data linkage of medical records research purposes, and if commercial organisations were to partake, certain obligations such as returning benefits to healthcare systems was preferred (Textbox 5).

ICE: “You do not give information to whomever. Or at least I do not. I have been involved in deCode genetics [centralised healthcare database], a study looking for high risk factors for a disease being looked for in a large family. Which, I feel is necessary

to take part in as it could be of benefit to others. (FG3, East of Iceland, P22, Male, aged 61-70)

Factors affecting trust and acceptance of health data sharing

A pattern of factors emerged affecting the acceptability for health data to be shared for secondary purposes in different contexts. The emerged themes were: a) information provision and individual-level control, b) responsibility and accountability, and c) fairness in data use, representation, and reciprocity.

3. Information provision and individual-level control

Health data flowing between different third parties on the internet was perceived by participants to be unrestricted, particularly with smartphone applications and internet searching. Participants regarded the main starting point of governance for secondary uses of health data was ensuring they were adequately informed of the handling of data and use purposes. This should apply even in situations where consent could not be obtained, such as if the data were anonymised. Not being informed was perceived negatively and affected willingness to share data (Textbox 6).

SWE: "They [third parties] use me, even though I don't know about it and even if they use it for a good purpose, they still use me ... even though it [data] is decoded and nobody will know [me]. No, I feel like it is not okay. It would have been better if I had been told what will happen ... So, I think some kind of information before sharing..."

(FG1, Sala, P3, Female, aged 41-50)

Many participants wanted to be part of the decision-making process for the reuse of their health data in and outside of healthcare. Notably some wanted to be asked to consent, at the

point when the data was re-used if this was appropriate and manageable. Others felt that information and clarity provided some sense of control for individuals, and the lack of information facilitated mistrust and helplessness (Textbox 7).

SWE: "For my part, it is sufficient that I will be informed and then that I can reach them if I have questions or comments. I don't feel like I need to approve/consent, but still maybe ...if they could tell: just so you know, this is going to happen." (FG2, Sala, P9, Female, aged 18-30 Women, No9, Reference 22896 – 23112, Sweden)

Some participants called for clarity over data subject's rights, as they imagined data flows to be complex due to the changeable contexts health data may be reused in, the third parties involved and their intentions, and the level of identifiability (Textbox 8).

ENG: "Who actually owns the data? ...Whether it should belong to National Health [Service], should it belong to the individual, how's it going work, particularly with all the data advances in genetics, and all things they'll be able to find out in the foreseeable future? ... that's going to be quite complicated...and who's got rights." (FG1, Oxford, P04, Male, aged 61-70)

4. Oversight and accountability of health data re-use

Participants deliberated on ways in which health data could be responsibly shared and reused, as they perceived that absolute privacy could not be achieved in modern society, and benefits of sharing data sometimes outweighed the risks. Responsibility for ensuring optimal data disclosure practice was seen as a responsibility that was held by everyone along the approval and reuse chain. This also meant that data subjects should have responsibility to decide whether, and how to share data about themselves. English and Swedish participants wanted to be informed of future data use and profits made from health data, whereas the Icelandic participants wanted a centralised information and consenting system. Iceland's participants

argued for a system where they could consent to sharing their data for different purposes. According to all participants, governments are responsible for regulation and guidance, and data users and sharers naturally were obliged to uphold wishes of data subjects, act ethically and within the confines of the law (Textbox 9).

ENG: "Instead of playing catch-up all the time it would be really, really nice if the legal framework was in place first to build up public trust and then people will say that's fine. Make sure that the people who are in charge of securing data are qualified enough to be able to carry out what they're supposed to be doing." (FG1, Oxford, P07, female, aged 41-50)

Responsible data sharing involved the need for the right amount of oversight by parties involved in the handling of data and by regulatory bodies to enforce regulations and penalties. Some participants in England and Sweden expected heavier punitive actions for mishandling of data and breaches, relative to the responsible organisation's income and severity, such as fines and even imprisonment. This would hold those responsible for data sharing and reuse accountable for their practices. In Iceland, though participants did not mention repercussions, there was preference for traceability and accountability (Textbox 10).

ENG: "I'd feel more secure that they [data users] would be reprimanded if they were to do something wrong.... I'd feel more secure that they would be heavily reprimanded for it" (FG4, Manchester, P26, Male, aged 31-40)

Monitoring and limiting the reuse of data was suggested by participants as a legitimate solution to prevent misuse. Some suggested that those may reuse the data and the purposes for which it could be used should be limited, such as for medical research and informing health and social care services, as well as applying time limits for access and reuse (Textbox 11).

SWE: "It [the data] can only be read once, like in Mission Impossible." (FG3, Uppsala, P17, Male, 61-70)

The future re-use of data by private companies was something that participants felt was not currently being addressed adequately. In the English focus groups, the preference was for the data to be returned to the original collectors, most likely healthcare providers, and the benefits to be shared among stakeholders. It was regarded as important that when data was shared with third parties that this must be as close to the original agreement as possible. The Swedish participants were very hesitant to share data with companies stating desire for consent options (Textbox 12).

ENG: "I would want to know more information about what the tech company retain from that information and how it's safeguarded and is it passed back to the hospital, and they don't keep any of it or can they use it for their own development of future software for their company to then do whatever they want? I would want to know what exactly they're going to do with it in the future." (FG2, Oxford, P12, Female, aged 18-30)

5. Fairness in data use, representation and reciprocity

In sharing data with private companies, the question of fairness arose mainly in the English focus groups. It was suggested that a balance was required that met everyone's demands. There was recognition that data is needed for many purposes, but legislation needed to address fair use and protect from misuse (Textbox 13).

ENG: "How do you do it fairly and equitably and safely and yet still get the most out of this data? ... The problem is that I don't think you can really protect data, but you need legislation for it. For example...I can have the data, but I'm not allowed to use it maliciously." (FG1, Oxford, P07, Female, aged 41-50)

However, participants in Iceland viewed their experiences with deCODE positively due to the perceived fairness in data use and sharing.

ICE: “but here, decCODE Genetics. They have been calling people in. For a very general examination, naturally only with people’s consent. And they are just looking at everything about the people.” (FG2, Reykjavik, P13, Female aged 61-70)

Participants regarded that something should be given back to data subjects, healthcare providers, or that society should benefit in some way. Some participants explained they felt unfairness due to the lack of choice about what happens with their data, and the sharing and use should be proportionate to the benefit they receive from giving up their data (Textbox 13).

ENG: “Where I have a problem is where that data is then taken by private contractors, pharmaceutical companies, they make profits out of it. And they use... those profits don’t go back to all of us, that’s going to them and their shareholders. So, like you were saying, if the gains are distributed across the population who are providing that valuable data, then I have no problem.” (FG5, London, P19, Female, aged 31-40)

Experiences of and perceptions of the way in which health data was used to profile individuals or groups by private companies caused unease in some participants. Many assumed that they would be profiled based on the things they bought online or their internet searches, but the resulting marketing and advertising caught some participants by surprise. They did not know that data would be linked in so many ways, between third parties, or that data could be collected without the knowledge of data subjects. This was considered unfair for the purposes the data was reused for, and for some it removed the choice about how they would want to be represented online, if at all, and how genuine the profile was. Further anxiety about potentially being discriminated against, or experiencing harm, due to the assumptions companies make through profiling was also expressed (Textbox 14).

ICE: “Yes, people take part in these games on Facebook or play a game with a friend and then you have been profiled. And you are sent fake news or stories that directly affect you as a person ... So, I really think it makes a lot of difference who mixes big data.” (FG1, Reykjavik, P10, Male, aged 51-60)

Swedish participants doubted the ability to control the purpose of data use. Some expressed that profiling may have more impact on younger people, since over their life course more data and more profiling would occur. Therefore, data users needed to handle data appropriately, and in so doing ensure that it did not make discriminatory inferences nor create inequalities for data subjects (Textbox 14).

SWE: “...you do not want to be stigmatized [when you are young], but when you are seventy plus it does not matter so much anymore.” (FG4, Uppsala, P21, female, aged 71+)

For some English participants it was difficult to know who the authorities were to complain to and be heard when something went wrong. Participants not only called for more government oversight and legislation to protect individuals and society from risks posed by the potential continuous flow of their health data to commercial organisations, but also to understand better existing regulation in how it protects data and visibility of relevant authorities (Textbox 15).

ENG: “If we could lobby people to say somebody has to take this a little bit more seriously then maybe something will happen. ...people are complaining about a lot of things, and you just get ignored. The problem is people don't even understand what they're giving away so can't get upset about it to the extent that they might if they fully understood the problem. Nobody's out there trying to educate people.” (FG1, Oxford, P07, Female, aged 41-50)

Discussion

The analysis presented here focused on the common issues found in all of the study countries to reconcile the data trust deficit regarding secondary uses of health-related data. The core challenges related to the persistent lack of information and transparency in health data flows between contexts, the hope for ethical practice among commercial entities and stronger enforcement of legislation and penalties for the misuse of health data, and the equitable reciprocity from financial gain of commercial companies. Study participants focused primarily on the purpose and benefits of sharing data in contrast to maintaining privacy. Participants have clear expectations about what is appropriate use of their data.

Nissenbaum (30-32) stated that when data moves across contexts, i.e. used for different purposes than expected it violates personal boundaries. The study demonstrates that participants recognised the importance of contextual boundaries. Embedded in the healthcare context are feelings of trust and reciprocity – that people feel violated when third parties are involved. Similar to this study, Snell et al (43) found that national healthcare services were perceived to have better governance and therefore levels of trust when compared to commercial third parties. What is common to all health systems is that public-private partnerships seem essential for data-driven healthcare dependent on digital technology and innovation. Commercial companies typically provide the technological expertise and tools while healthcare partners pay for the service they need, which requires access to data. Commercial involvement involves a clash of different contexts and motivations and practices, however reconciling the norms and values should be a priority. The speed at which public-private contexts have been meeting has not provided enough time for good normative standards to be rigorously set (24). Data subjects' input and wishes are often not sought in these partnerships nor in commercial platforms that collect health data and share with other commercial third parties. This study shows that when contextual integrity is breached, citizens'

expectations are for their preferences for the handling of their health data to extend from trusted contexts such as healthcare to others with differing values. This means, the purposes and principles of data sharing should be consistently held from one context to another, with data subjects' reasonable expectations placed at the centre. Public entities should ensure this when negotiating data sharing agreements.

On regulation, there is a wealth of literature that points to confusion about the scope and efficacy of legal requirements (12, 13, 21). Glenn and Monteith (12) state that an increasing amount of user-generated health data in the United States falls outside of HIPAA protection, such as data from internet searches, smartphone apps, and social media. Pagliari (21) states that "issues of consent and legitimate interest are muddled in the multiparty data ecosystem of digital health apps", and the 'exploitative' behaviours that profile individuals and groups, may in the future affect access to healthcare and treatment (14, 21-23). While regulation to protect data exists in the EU, a recent Norwegian Consumer Council report highlighted exploitation of consumer data for profiling and advertising by the Advertisement-technology industry, and found that the majority of apps analysed were in breach of GDPR third party data transmission requirements (47). The lack of accountability and transparency about data flows and usage is a threat to privacy (14, 17, 21-23) and can in turn, endanger trust and any positive outcomes of data sharing. The participants understood that there are regulations and rights in place in the EU for data protection and sharing. However, the findings have notable implications for regulation and practice - several areas where governance needs to improve or provide better choice to citizens were suggested by participants. These included improved effort to provide better information about data sharing practices in privacy policies on all digital platforms including wearables, mHealth apps, and by public-private collaborations, choice in level of identifiability of data subjects, and governance also of anonymous information.

A key finding was the call for reciprocity in the English focus groups from data shared with commercial entities, in that individuals, research and health services in general should receive

direct benefits for data shared that aided profit-making. In Iceland, participants stated that reciprocity meant something good coming out of the use of data and was what made sharing with deCODE acceptable to them (see 48). Though, for individual benefits to be returned would require the identification of individuals whose data were used and cannot be possible when using anonymised data sets. However, in the interests of fairness, clarity of the benefit returns could form part of data acquisition processes and potentially be a welcome condition in approval processes from a public viewpoint. Finally, ensuring that legislation, enforcement, and punishment are severe to prevent data misuse would reassure data subjects and was an important factor for trust in governance. While some of the suggested improvements reveal a gap between the law and how it is practiced or perceived to be, other suggested improvements constitute a significant leap from the GDPR, such as the request for governance of anonymous data and group protection.

Limitations

There were more middle to older aged category adults, and Iceland which had a bigger age difference in the sample. The samples were recruited differently in the countries, both England and Sweden recruited using convenience methods and Iceland through the national population register selecting contacts at random. Convenience sampling and snowballing may have introduced selection bias, meaning results may not generalise well to the study country populations, and future research should aim to minimise this bias through recruiting representative samples. While all researchers were fluent in English, not all spoke Swedish and/or Icelandic, and as such the researchers aimed to capture the commonalities across the data rather than the cultural and semantic differences, which were more difficult to disclose as a result.

Conclusion

Data governance policy should involve public perspectives on an ongoing basis and inform and implement changes to data use and sharing practices coinciding with public views. Where

public-private partnerships are created, or in instances where data crosses contextual boundaries, entities receiving data should operate within the rules and social expectations of the healthcare context. The core ideals included data to be used for ethical purposes even when there was commercial interest, data subjects and/or public institutions that provide and share data should receive benefits from the sharing of data, control over data sharing requires more transparency and clarity over accountability, and information provision helps to empower data subjects. Future research should aim to develop mechanisms for these preferences.

Authorship

NS and JVJ designed the study with feedback from DM, JK, SC, HBB, GAJ and Jorien Veldwijk. NS, JVJ and EH conducted and analysed the focus groups and interpreted the data with the research team including DM, JK, HBB, SC, and GAJ. NS drafted the article and all co-authors reviewed it.

Acknowledgements

This article reports research conducted as part of the project “Governance of Health Data in Cyberspace”. The project is a joint undertaking between the University of Oxford, the University of Iceland, Uppsala University and the University of Oslo. In addition to the named authors, the following individuals have contributed to the article through group discussion, peer support and research document review: Professor Lee Andrew Bygrave, Dr Jorien Veldwijk, Kristine Beitland, and Professor Joe Cannataci. Thanks to Guðbjört Guðjónsdóttir for co-running the focus groups in Iceland.

Funding

This work was supported by NordForsk [grant number 81105] and the Economic and Social Research Council (part of UK Research and Innovation)

Conflict of interest

None declared.

Summary Table

What was already known on the topic?

- Digital technologies are becoming the backbone for a data-driven health sector
- The possibility to link patient data to commercial data such as insurance and purchasing habits may help better understand individual health, behaviours and lifestyle.
- There is confusion about the scope and efficacy of legal requirements for secondary uses of health data in cyberspace
- A data trust deficit exists in society and health data sharing for secondary purposes requires public dialogue

What this study added to our knowledge?

- Participants declared that acceptability of secondary use of health data depends on purpose
- Citizens perceived lack of control over how their health data proliferates in cyberspace
- Improving public awareness about health data flows and their data rights will better equip data subjects when making data sharing decisions, particularly when considering trade-offs
- Call for fairness in use, data subjects' preferences should be better represented in data sharing decisions, and reciprocity of benefits when health data is shared with third parties

References

1. OECD (2013). Strengthening Health information infrastructure for health care quality governance: Good practices, new opportunities, and data privacy protection challenges. OECD Health Policy Studies, OECD Publishing. <https://www.oecd.org/publications/strengthening-health-information-infrastructure-for-health-care-quality-governance-9789264193505-en.htm>
2. OECD (2015). Health Data Governance: Privacy, Monitoring and Research. OECD Health Policy Studies, OECD Publishing. https://www.oecd-ilibrary.org/social-issues-migration-health/health-data-governance_9789264244566-en
3. Topol, E.J. (2019). Preparing the healthcare workforce to deliver the digital future. <https://topol.hee.nhs.uk/wp-content/uploads/HEE-Topol-Review-2019.pdf>
4. Castell, S., Robinson, L., Ashford, H. (2018) Future data-driven technologies and the implications for use of patient data Dialogue with public, patients and healthcare professionals. <http://www.ipsos-mori.com/terms>.<http://www.ipsos-mori.com/terms>.
5. Skovgaard, L. L., Wadmann, S., Hoeyer, K. A. (2019). Review of attitudes towards the reuse of health data among people in the European Union: The primacy of purpose and the common good. *Health Policy*, 123, 564–71. <https://doi.org/10.1016/j.healthpol.2019.03.012>
6. Pastorino, R., De Vito, C., Migliara, G., Glocker, K., Binenbaum, I., Ricciardi, W., Boccia, S. (2019). Benefits and challenges of Big Data in healthcare: an overview of the European initiatives. *European Journal of Public Health*, 29(3), 23–7. <https://doi.org/10.1093/eurpub/ckz168>
7. Science and Technology Advisory Council (2014). The Future of Europe is Science. European Commission Report. https://ec.europa.eu/archives/commission_2010-2014/president/advisory-council/documents/the_future_of_europe_is_science_october_2014.pdf
8. Ipsos MORI for Wellcome Trust (2016). The One-Way Mirror: Public attitudes to commercial access to health data. https://wellcome.figshare.com/articles/journal_contribution/The_One-Way_Mirror_Public_attitudes_to_commercial_access_to_health_data/5616448/1
9. The Academy of Medical Sciences Report (2018). New technologies that use patient data. <https://acmedsci.ac.uk/file-download/77418765>
10. Kalkman, S., Van Delden, J., Banerjee, A., Tyl, B., Mostert, M., Van Thiel, G. (2019). Patients' and public views and attitudes towards the sharing of health data for research: A narrative review of the empirical evidence. *Journal of Medical Ethics*, Nov 12. doi:10.1136/medethics-2019-105651
11. Whiddett, R., Hunter, I., Engelbrecht, J., Handy, J. (2006). Patients' attitudes towards sharing their health information. *Int J Med Inform.* 75, 530–41. <https://doi.org/10.1016/j.ijmedinf.2005.08.009>
12. Glenn, T., Monteith, S. (2014). Privacy in the Digital World: Medical and Health Data Outside of HIPAA Protections. *Current Psychiatry Reports*. 16:494. <https://doi.org/10.1007/s11920-014-0494-4>
13. Powell, A.C., Singh, P., Torous, J. (2018). The Complexity of Mental Health App Privacy Policies: A Potential Barrier to Privacy. *JMIR mHealth uHealth*. 6(7):e158. <http://mhealth.jmir.org/2018/7/e158/>

14. Grundy, Q., Chiu, K., Held, F., Continella, A., Bero, L., Holz, R. (2019). Data sharing practices of medicines related apps and the mobile ecosystem: Traffic, content, and network analysis. *BMJ*. Mar 20:364. <https://doi.org/10.1136/bmj.l920>
15. Blenner, S.R., Köllmer, M., Rouse, A.J., Daneshvar, N., Williams, C., Andrews, L.B. (2016). Privacy Policies of Android Diabetes Apps and Sharing of Health Information. *JAMA*. 315(10):1051. <http://jama.jamanetwork.com/article.aspx?doi=10.1001/jama.2015.19426>
16. Zang, J., Dummit, K., Graves, J., Lisker, P., Sweeney, L. (2015), Who Knows What About Me? A Survey of Behind the Scenes Personal Data Sharing to Third Parties by Mobile Apps. *Technology Science*. <http://techscience.org/a/2015103001>
17. Steinhubl, S.R., Muse, E.D., Topol, E.J. (2013). Can Mobile Health Technologies Transform Health Care? *JAMA*. 310(22):2395–2396. <http://jama.jamanetwork.com/article.aspx?doi=10.1001/jama.2013.281078>
18. Lang, M., Knoppers, B.M., Zawati, M.H. (2020). International mHealth Research: Old Tools and New Challenges. *J Law Med Ethics*. 48(1):178–86. <http://journals.sagepub.com/doi/10.1177/1073110520917045>
19. Dobos, L. (2018, February 18). 2.7 million recorded calls to 1177 Vårdguiden completely unprotected on the internet. *Computer Sweden*. <https://computersweden.idg.se/2.2683/1.714787/inspelade-samtal-1177-varldguiden-oskyddade-internet>
20. Wadmann, S., Hoeyer, K. (2018). Dangers of the digital fit: Rethinking seamlessness and social sustainability in data-intensive healthcare. *Big Data and Society*. 5(1). <https://doi.org/10.1177%2F2053951717752964>
21. Pagliari, C. (2019). Commercial health apps: in the user's interest? *BMJ*. Mar 21; 364:l1280. <https://doi.org/10.1136/bmj.l1280>
22. Dehling, T., Gao, F., Schneider, S., Sunyaev, A. (2015). Exploring the Far Side of Mobile Health: Information Security and Privacy of Mobile Health Apps on iOS and Android. *JMIR Mhealth Uhealth*. 2015;3(1):e8. DOI: 10.2196/mhealth.3672
23. Sunyaev, a., Dehling, T., Taylor, P.L., Mandl, K.D. (2015). Availability and quality of mobile health app privacy policies. *Journal of the American Medical Informatics Association*. 22(e1):e28–e33. <https://doi.org/10.1136/amiajnl-2013-002605>
24. Ballantyne, A., Stewart, C. (2019). Big Data and Public-Private Partnerships in Healthcare and Research. *Asian Bioeth Rev*. 11(3):315–26. <https://link.springer.com/article/10.1007/s41649-019-00100-7>
25. ICO (2017). Royal Free - Google DeepMind trial failed to comply with data protection law. Jul 3. <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law/>
26. Miltgen, C.L., Peyrat-Guillard, D. (2014) Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. *Eur J Inf Syst*. 23(2):103–25. <https://orsociety.tandfonline.com/doi/abs/10.1057/ejis.2013.17>

27. Riordan, F., Papoutsis, C., Reed, J.E., Marston, C., Bell, D., Majeed, A. (2015). Patient and public attitudes towards informed consent models and levels of awareness of Electronic Health Records in the UK. *Int J Med Inform.* 84(4):237–47. <http://dx.doi.org/10.1016/j.ijmedinf.2015.01.008>
28. Spencer, K., Sanders, C., Whitley, E.A., Lund, D., Kaye, J., Dixon, W.G. (2016). Patient Perspectives on Sharing Anonymized Personal Health Data Using a Digital System for Dynamic Consent and Research Feedback: A Qualitative Study. *J Med Internet Res.* 18(4):e66. <http://www.ncbi.nlm.nih.gov/pubmed/27083521>
29. Patil, S., Lu, H., Saunders, C.L., Potoglou, D., Robinson, N. (2016). Public preferences for electronic health data storage, access, and sharing — evidence from a pan-European survey. *J Am Med Informatics Assoc.* 23(6):1096–106. <https://academic.oup.com/jamia/article-lookup/doi/10.1093/jamia/ocw012>
30. Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review.* 79(1):119-158. <https://core.ac.uk/download/pdf/267979739.pdf>
31. Nissenbaum, H. (2009). Privacy in context: Technology, policy, and the integrity of social life. Stanford: Stanford University Press.
32. Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Daedalus.* Fall issue. <https://www.amacad.org/publication/contextual-approach-privacy-online>
33. Shklovski, I., Mainwaring, S.D., Skúladóttir, H.H., Borgthorsson, H. (2014). Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.* Apr: 2347-2356. <https://doi.org/10.1145/2556288.2557421>
34. Barkhuus, L. (2012). The Mismeasurement of Privacy: Using Contextual Integrity to Reconsider Privacy in HCI. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.* May:367-376. <https://doi.org/10.1145/2207676.2207727>
35. Papoutsis, C., Reed, J.E., Marston, C., Lewis, R., Majeed, A., Bell, D. (2015) Patient and public views about the security and privacy of Electronic Health Records (EHRs) in the UK: results from a mixed methods study. *BMC Med Inform Decis Mak.* 15(1):86. <https://doi.org/10.1186/s12911-015-0202-2>
36. Wellcome Trust (2013). Summary Report of Qualitative Research into Public Attitudes to Personal Data and Linking Personal Data. <https://wellcomecollection.org/works/am3zpgqv>
37. Lehnborn, E.C., Mclachlan, A.J., Brien, J.A.E. (2013). A qualitative study of swedes' opinions about shared electronic health records. In: *Studies in Health Technology and Informatics.* IOS Press.
38. O'Doherty, K.C., Christofides, E., Yen, J., Bentzen, H.B., Burke, W., Hallowell, N., et al (2016). If you build it, they will come: unintended future uses of organised health data collections. *BMC Med Ethics.* 17(1):54. <https://doi.org/10.1186/s12910-016-0137-x>
39. Kim, K.K., Browe, D.K., Logan, H.C., Holm, R., Hack, L., Ohno-Machado, L. (2014). Data governance requirements for distributed clinical research networks: triangulating perspectives of diverse stakeholders. *J Am Med Informatics Assoc.* 21(4):714–9. <https://doi.org/10.1136/amiajnl-2013-002308>
40. Royal Statistical Society (2014). Research on trust in data and attitudes toward data use / data sharing. <https://www.statslife.org.uk/images/pdf/rss-data-trust-data-sharing-attitudes-research-note.pdf>

41. The Royal Society (2017). Data management and use: governance in the 21st century. https://royalsociety.org/~media/policy/Publications/2017/Data_management_and_use_governance_in_the_21st_century_2017_seminar_report.pdf
42. Shah, H. (2017). The DeepMind debacle demands dialogue on data. *Nature*. 547:259. <https://doi.org/10.1038/547259a>
43. Snell, K., Starkbaum, J., Lauß, G., Vermeer, A., Helén, I. (2012). From protection of privacy to control of data streams: a focus group study on biobanks in the information society. *Public Health Genomics*. 15(5):293–302. <https://doi.org/10.1159/000336541>
44. National Data Guardian (2018). A report of a citizens' jury designed to explore when it is reasonable for patients to expect patient data to be shared. <https://www.connectedhealthcities.org/wp-content/uploads/2018/08/Reasonable-expectations-jury-report-v1.0-FINAL-09.08.18.pdf>
45. Bradley, E.H., Curry, L.A., Devers, K.J. (2007). Qualitative data analysis for health services research: developing taxonomy, themes, and theory. *Health Serv Res*. 42(4):1758–72. <https://doi.org/10.1111/j.1475-6773.2006.00684.x>
46. Pope, C., Ziebland, S., Mays, N. (2000). Qualitative research in health care. Analysing qualitative data. *BMJ*. 320(7227):114–6. <https://doi.org/10.1136/bmj.320.7227.114>
47. Norwegian Consumer Council (2020). REPORT: Out of Control: How consumers are exploited by online advertising industry. <https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/report-out-of-control/>
48. Gulcher, J., Stefansson, K. (1999). An Icelandic saga on a centralized healthcare database and democratic decision making. *Nat Biotechnol*. 17, 620. <https://doi.org/10.1038/10796>

Appendix A: Socio-demographic questionnaire

Governance of health data in cyberspace: Participant survey

Thank you for taking part in this study. We would like to ask you some questions about your background. This will help us to understand who has taken part in the study.

It will take approximately 3 minutes to complete.

Taking part in this survey is **voluntary**, your answers are strictly anonymous and will be kept confidential. You can decline to answer any questions you do not want to. We will not be able to identify you from this information.

If you decide not to complete this survey, you can still take part in the focus group.

1. What is your gender?	2. How old are you? (years)
<input type="radio"/> Male <input type="radio"/> Female <input type="radio"/> Other <input type="radio"/> Prefer not to say	<input type="radio"/> 18 – 30 <input type="radio"/> 31 – 40 <input type="radio"/> 41 – 50 <input type="radio"/> 51 – 60 <input type="radio"/> 61-70 <input type="radio"/> 71+ <input type="radio"/> Prefer not to say

3. What is your highest level of education?	4. Have you ever had a job that was related to health, research, or using data in some way?
<input type="radio"/> Less than secondary / high school <input type="radio"/> Secondary / high school <input type="radio"/> Vocational/professional qualifications <input type="radio"/> Bachelor's degree <input type="radio"/> Postgraduate degree <input type="radio"/> Other <input type="radio"/> Prefer not to say	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Prefer not to say

5. What is your ethnic group?

☐ White (English/Welsh/Scottish/Northern Irish/British)

☐ White Other

Mixed/Multiple groups

☐ White and Black Caribbean

☐ White and Black African

☐ White and Asian

☐ Any other mixed/multiple ethnic background

Asian/Asian British

☐ Indian

☐ Pakistani

☐ Bangladeshi

☐ Chinese

☐ Any other Asian background

Black/African/Caribbean/Black British

☐ African

☐ Caribbean

☐ Any other Black/African/Caribbean Background

Other ethnic group

☐ Arab

☐ Any other ethnic group

☐ Prefer not to say

6. Which of the following devices, if any, have you used? (Tick all that apply)	7. How often do you use the internet?
<input type="radio"/> Desktop computer <input type="radio"/> Laptop <input type="radio"/> Smartphone <input type="radio"/> Tablet <input type="radio"/> Smartwatch <input type="radio"/> Other (please specify) <hr/> <input type="radio"/> Prefer not to say	<input type="radio"/> Once a day <input type="radio"/> More than once a day <input type="radio"/> A few times each week <input type="radio"/> A few times a month <input type="radio"/> Less than once a month <input type="radio"/> Never <input type="radio"/> Prefer not to say

8. How often do you use mobile applications?	9. Have you ever used a mobile health application for e.g. to track your health or lifestyle?
<input type="radio"/> Once a day <input type="radio"/> More than once a day <input type="radio"/> A few times each week <input type="radio"/> A few times a month <input type="radio"/> Less than once a month <input type="radio"/> Never <input type="radio"/> Prefer not to say	<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> I don't know <input type="radio"/> Prefer not to say

Thank you for taking the time to complete this survey. Please return the completed survey back to the researchers who are running the focus group.

Appendix B: Focus groups discussion guide

Focus group discussion guide

Opening questions – warm up round	
1a.	<p>To start with, I would like you to think about the things you do online, the digital devices that you may use or come across, and then to describe what happens if and when you are asked to provide information about yourself in different situations. Tell me about your experience.</p> <p>PROMPT: How often do you use the internet, buy things online, use smartphone or tablet apps, use the internet on a computer/smartphone/iPad, communicate using Twitter or FB, or use customer loyalty cards?</p> <p>PROMPT: What kinds of information do you provide? E.g. name, bank details, email address, photographs, physical information etc.</p>
1b.	<p>Now I would like you to think about the information or data you might have to provide when you visit your doctor or the hospital.</p>
1b.i	<p>What kinds of information, do you think that healthcare professionals routinely collect about their patients? (without giving any health information about yourself)</p> <p>Prompt: test results, medical history, health behaviours e.g. diet or exercise etc.</p>
1b.ii	<p>Do you think that your health data is used for other healthcare purposes, not just your own care? If so, what are these?</p> <p>Prompt: to help treat other people, and make services better etc.</p>
Introduction to Governance concepts	
<p>Our society has different types of controls in place to govern and safeguard how health data is used, shared, accessed, and protected. These controls include laws, regulations, asking people for consent, or panels or groups that decide about access control and give permissions. Other controls might include oversight from different authorities, and there are also rules that are specifically about how data should be handled at the point of capture, storage and access.</p>	
2a.	<p>Thinking about the times you are asked to provide information or when data is captured about you, can you tell me if you are aware of any controls or safeguards that protect your health data in healthcare? What do you think these are?</p> <p>Prompt: asking me about using my data, healthcare professionals/clinics/hospitals to keep my data confidential and secure, only authorized people are able to use my data, GDPR / data protection act, terms and conditions etc.</p>
2b.	<p>In your opinion, who is responsible for ensuring health data is shared and reused in a way that you expect in healthcare?</p> <p>Prompt: Is it you? Who else?</p>
2c.	<p>Are there different people responsible for how your health data is shared and reused outside of healthcare?</p>

	Prompt: Law makers/politicians; companies who use my data, other etc.
--	---

Key questions – Important aspects for people	
<p>I will now ask you to consider three scenarios about how health data or information might be shared and used in different situations for different purposes. The narrative follows Tina, a woman who is 38 years old. Just to note that the person in the scenarios is not a real person. After I read you the scenarios, I will ask you questions about your impressions. There are no right or wrong responses, we are just asking for your views.</p>	
<p>Tina is admitted to hospital and has various medical tests, and sees different healthcare professionals. She also has a genetic test to determine which type of illness she is suffering from. The doctors and nurses have to record all clinical information and notes about her into the electronic health record system, such as her symptoms, reason for admission, her medical history, her family's medical history, prescriptions, her medical test results including x-ray and MRI images, DNA sequences, and diagnosis and treatment plan.</p> <p>[Tina's medical test results include genomic data. This is genetic information that is unique to Tina and can never be fully de-personalised. It is also very similar to the genetic information of her relatives and could be used to link her data to theirs, or to infer their risk of developing a disease.]</p> <p>By sharing all of the test results in Tina's health record with each other, the healthcare professionals in the hospital diagnose her with a long term medical condition.</p> <p>The hospital must report some health results to the national health authorities, so they can monitor the health issues of the population.</p> <p>An example of public health datasets are cancer registries which have a record of all people who have had cancer in the country. The data can also be linked to other government datasets such as death records. Local government, health services and researchers from universities and companies can access these public health datasets, if they can demonstrate a worthwhile purpose.</p> <p>Tina's hospital admission data including test results is shared by the hospital with the national health authority as part of the routine collection.</p>	
3a.	<p>Do you expect patient data to be shared with the national health authorities? Is it okay that local government, and research professionals can also use it? Can you explain why?</p> <p>PROMPT: Do any of the following matter and can you give examples?</p> <ul style="list-style-type: none"> Who data is shared with – in this case its local/national authorities and professionals What types of data are shared Purposes of reusing the data Level of identifiability What controls / safeguards are in place
3b.	<p>Who do you think has a role or responsibility for ensuring how patient data is shared and used? What, if any, would you want your role to be?</p>

	PROMPT – Do you think you should give consent or receive information about the data use every time?
<p>Several months after Tina is discharged from the hospital, she hears on the news that a global technology company has developed new software that uses artificial intelligence to help doctors diagnose and treat patients with her particular disease by combining and learning from data included in patient’s electronic health records.</p> <p>[AI is the field which creates intelligent machines, and it requires massive amounts of data to be able to draw conclusions about things].</p> <p>The hospital and technology company had made a data sharing agreement to test out the software. The tech company is using patients’ data from the hospital’s patient electronic records where Tina was admitted. It is not clear to patients what data was shared. Data was shared between the hospital and technology company without patients’ knowledge. However, the data that was shared was de-identified, meaning information such as name, DOB, address etc. that would identify the patients was removed.</p> <p>The hospital and doctors will use this AI software to understand how to diagnose and treat new patients who are admitted with similar medical problems as Tina.</p>	
4a.	<p>In your opinion, was it acceptable for patient data to be shared in this way? Can you explain why?</p> <p>PROMPT: depends on which data is used, why it is used, what security is in place, why patients were not informed, patients should have been asked, I don’t want a tech company to know my data etc., OR as long as data is kept confidential, as long as its improving healthcare etc.</p> <p>[You mentioned it depends on what data was shared, how much does this matter? Even if name and address were removed, but your DNA sequence data was shared – does that matter?]</p>
4b.	<p>What, if any, expectations do you have for how the data should be shared and handled in this situation?</p> <p>PROMPT: Under what conditions should the global tech company comply? You mentioned that it is important for you that [e.g. the hospital asks for your permissions; only authorised people can use the data, only if data is de-identified, that data is kept secure, data is not misused], can you tell me more about that?</p>
4c.	<p>Who has a role or responsibility for ensuring how patient data is shared and used? What, if any, would you want your role to be?</p> <p>PROMPT – Do you think you should give consent or receive information about the data use every time?</p>
<p>Tina’s condition requires daily monitoring at home through the use of medical devices such as a blood pressure monitor that can prompt her when she should seek medical advice, or through applications on her smartphone or smartwatch (FitBit or AppleWatch) that gather data about the status of her health. These devices store their data online. Tina also uses applications on her</p>	

smartphone to keep track of her weight, eating and exercise behaviours, separate from monitoring her health condition, but to lead a healthy lifestyle. This is called health-relevant data or lifestyle data.

The health-relevant data Tina collects is stored by the smartphone company and apps used, and cannot be seen by Tina's healthcare provider/doctor. Tina and other users can see their data at any time.

The Smartwatch company and other devices and applications use some or all data collected from Tina and other consumers to improve the way their software and services work.

The companies could also sell access to some, or all, of the consumers' information to other companies or organisations known as third parties, so long as the consumers are informed that this might happen in the Terms and Conditions of use.

Third party companies and app developers may also be given access to the data for different purposes such as marketing and advertising, and they may collect health-relevant data on individuals from different places.

One such third party company (a mobile health app) collects data on Tina from the smart devices that monitor her health and lifestyle. The company uses the data to advertise health products to Tina, help her to connect with relevant social media groups, and individually tailor the service she receives.

Other potential users of the data from such applications and smart devices might include researchers or universities, or pharmaceutical companies. They might use it for a number of different purposes such as research for identifying health trends across the population.

5a.i	In your opinion, is it acceptable for health-relevant and lifestyle data to be used within the company for improving services? Can you explain why?
5a.ii	<p>Is it acceptable for health-relevant and lifestyle data to be shared with third parties in this way? Does it matter what kind of organisation the third party is, or what the purpose is? Can you explain further?</p> <p>PROMPT: depends on which data is used, why it is used, what security is in place, why patients were not informed, patients should have been asked, I don't want some companies to know my data etc., OR as long as data is kept confidential, as long as its improving healthcare etc.</p> <p>Would your answer be different if it were a public authority?</p>
5a.iii	<p>Can you give me examples of anyone or any organisation with whom you think would be acceptable to share this data? And what purposes are acceptable?</p> <p>PROMPT: Doctor, scientists, universities, national health authority, and pharmaceutical company etc. / for research improving my health and society's health, developing new treatments, evaluating healthcare provision etc.</p>
5b.	Under what conditions should the third party comply with? What, if any, expectations do you have for how the data should be shared in this situation?

	<p>PROMPT: What, if any, controls or safeguards do you think should be in place? [E.g. you mentioned that you look at the T&Cs? Or removing personal identifiable information, and only relevant information is shared, only approved or authorised people can use the data etc.] Can tell me more about that?</p> <p>Who has a role or responsibility for ensuring this data is shared and used? Do you think you have a role?</p> <p>PROMPT – Do you think you should give consent or receive information about the data use every time?</p>
--	--

<i>End questions – enable participants to reflect back on previous comments</i>	
6.	<p>We have now discussed your thoughts about sharing information about your health digitally. What are your take-away thoughts?</p> <p>PROMPT: Considering all of the scenarios we have discussed, what are your preferences for how your data might be shared and handled? How much control do you want to have?</p>
7.	<p>Will you think differently about how your information about your health is used?</p>
<i>Summary questions – capture if we missed something very important</i>	
8.	<p>Is there anything that we have not discussed, that you would like to mention?</p>