

Personal Data Store Ecosystems in Health and Social Care

Preprint | Commentary paper | v0.1 | 17 October 2023

Authors: Laura Carmichael^{1*}, Wendy Hall², Michael Boniface¹

¹ IT Innovation Centre part of the Digital Health and Biomedical Engineering Research Group, School of Electronics and Computer Science, University of Southampton, UK

² Web Science Institute, School of Electronics and Computer Science, University of Southampton, UK

* Corresponding author: L.E.Carmichael@soton.ac.uk

Licence

This preprint is available under a [Creative Commons Attribution License \(CC BY\)](#).
Copyright © the authors 2023.

Funding statement

This study was partly funded by the NIHR Southampton Biomedical Research Centre (NIHR203319) as part of the Data, Health and Society theme. The views expressed are those of the authors and not necessarily those of the National Institute for Health and Care Research (NIHR) or the Department of Health and Social Care.

Abstract

This paper considers how the development of personal data store ecosystems in health and social care may offer one person-centred approach to improving the ways in which individual generated and gathered data — e.g., from wearables and other personal monitoring and tracking devices — can be used for well-being, individual care, and research. Personal data stores aim to provide safe and secure digital spaces that enable people to self-manage, use, and share personal data with others in a way that aligns with their individual needs and preferences. A key motivation for personal data stores is to give an individual more access and meaningful control over their personal data, and greater visibility over how it is used by others. This commentary discusses meanings and motivations behind the personal data store concept — examples are provided to illustrate the opportunities such ecosystems can offer in health and social care, and associated research and implementation challenges are also examined.

Keywords

Data Donation; Data Governance; Data Portability; Personal Data Store Ecosystems; Personal Data Sovereignty; Privacy-by-Design; Self-Managing Data

1. Introduction

The wide-spread availability and use of wearables and other personal monitoring and tracking devices for health and wellness has increased opportunities for people to gather, collect, generate, and analyse data about themselves. Some examples being “personal genomics testing; diagnostic apps; and fitness, diet, and menstrual trackers” (1), which can be viewed as generating types of “participatory personal data” (2). There are various reasons why an individual may decide or may be compelled, to gather and generate data. For example, in some cases, a person may choose to do this for their own purposes (e.g., to work towards certain fitness goals), and then elect to share their data with peers for support (3). In other cases, a person may be expected or incentivised by others (e.g., insurers, clinicians) to engage in such activities — for instance, as part of a medical rehabilitation programme (3). Of course, it must be emphasised that not everyone makes the choice to actively collect, generate, or gather such data about themselves — or even has access to, or the necessary support to effectively use such technologies. However, the amount and variety of individual-generated data is only expected to grow, especially with increasing cyber-physical integration across all sectors of society [e.g., (4, 5)] — e.g., consider the potential for an increasing number of “smart monitoring devices [...] built into everyday appliances” (6), or for a majority of smartphones to feature inbuilt sensors and automatically installed health applications (7).

Yet, for many “individuals”, “health systems” and “researchers”, these person-generated data are often “not readily accessible” (8) — despite the right to data portability, which has been under-utilised in practice [see (9, 10)]. Attention is on how data practices across health and social care can be advanced to make better usage not only of traditional data flows, but also those emerging from this progressive digitalisation and datafication of health (11, 12).

Enabling individuals “to contribute personal data” safely and securely, where they should want to do so, is recognised as an important aspect of “secondary use of health data” that encourages “patient and public participation” (13). For example, approaches are needed that can better facilitate the sharing of “individual-generated data from monitors, wearables and trackers” with clinicians for individual care and with researchers (14).

In this paper, we specifically consider one type of socio-technical innovation: the development of trustworthy personal data store ecosystems, as a person-centred approach for helping to improve the use of individual generated and gathered data for well-being, individual care, and research. First, we discuss meanings and motivations for using personal data stores. Second, we outline examples to illustrate some of the opportunities personal data store ecosystems can offer in health and social care. Third, we explore research and implementation challenges associated with the development of such ecosystems. This commentary aims to prompt further conversation around the implications of developing trustworthy personal data ecosystems in health and social care — specifically the extent to which such an approach may contribute to more participatory data practices [e.g., see (12, 15)] — and to encourage further research and development in this area.

2. What are personal data stores?

Personal data stores can be viewed as a type of privacy enhancing technology (16, 17) that aim to provide safe and secure digital spaces, which enable people to self-manage, use, and share their personal data with others in a way that aligns with their individual needs and preferences (18). Effective and appropriate data controls and services are required [e.g., see (19)] so that a personal data store can be used by an individual for self-managing their personal data for their own personal use [e.g., for personal data generation, data portability, personal analytics, data retention, data deletion], and for consenting to secondary use by others [e.g., for permissioning, data access, monitoring re-usage, de-identification].

2.1. Motivations

In the “current attention economy” (20), conventional data models and practices are typically “organisation-centric” (21) — in that, much of the personal data (e.g., behavioural data) that people generate when online is collected, held and exploited by big data platforms in ways often invisible to them (20). Whereas personal data store ecosystems assume the form of more person-centred data models and practices [e.g., (21)], aiming to foster greater “personal data sovereignty” (22, 23, 24) — that is, giving individuals more access and control over their personal data, and greater visibility over how it is used by others. Such individual control should be “meaningful” (19) in the sense that people are able to determine how their personal data (as part of their personal data stores) can be accessed and used by others within safe and secure data ecosystems, and how such secondary uses may be of benefit to themselves and others. Seeing that individuals are increasingly becoming both active consumers and producers of personal data (25), the personal data store approach enables people to be more than passive data subjects (5). The expectation being that greater use of personal data stores will incentivise the development of new data-related services for users and encourage people to share more data for individual and societal benefit (22, 23).

Despite a diverse range of personal data store initiatives — e.g., BBC Box¹, Hub of All Things², Mydex³, Solid⁴ — personal data stores are yet to be widely adopted and used. However, the development of data spaces, marketplaces and other innovative approaches to personal data sovereignty remains a key area of interest for governments, industry and the public sector. For instance, giving individuals greater control over their personal data is one of the ambitions for the proposed EU European Health Data Space Regulation (26, 27); and for smart data schemes development in terms of consumer data [see e.g., (28)].

¹ Available at: <https://www.bbc.co.uk/rd/projects/databox> (Accessed October 3, 2023).

² Available at: <https://www.hubofallthings.com/> (Accessed October 3, 2023).

³ Available at: <https://mydex.org/> (Accessed October 3, 2023).

⁴ Available at: <https://www.inrupt.com/solid> (Accessed October 3, 2023).

3. Using personal data stores in health and social care

Four illustrative examples of how personal data stores might be utilised to help improve the ways in which individual-generated data can be used for well-being, individual care and research are now presented:

- Using data within **health and well-being apps**.
- Using data for **individual care**.
- **Donating data** for health and social care research.
- **Participating** in health and social care research.

These examples are by no means exhaustive but serve to highlight some of the opportunities that personal data stores can offer in the context of health and social care.

3.1. Using data within health and well-being apps

Personal health data are already being accessed, collected and generated by many individuals through different types of task specific apps for health and wellness. This includes those offered by healthcare providers [e.g., see NHS App,⁵ My Medical Record⁶] and others provided by technology companies [e.g., fitness trackers]. People may want to use their personal data stores to bring data from different health networks, apps and devices together in one place and to use their data in accordance with their individual needs and preferences.

Given that people often switch between apps, devices and technology providers, the use of personal data stores for data archival can also help to ensure that people do not lose access to data as technologies are replaced or become non-operational or obsolete [e.g., (29)]. Such a user-centric approach (22, 23) to data access, management and reuse may also help to drive the creation of and connection to other health and well-being services [e.g., for individual care, data donation] and increase the usability of existing apps [e.g., through enhanced mechanisms for data portability].

3.2. Using data for individual care

Personal data stores can provide one way in which people can share a wide-range of individual-generated data with health and social care professionals responsible for their care (30). By way of illustration, such services may provide patients with digital tools for “automatic form filling” and for communication of their “health story” with those responsible for their care to avoid unnecessary repetition (30).

3.3. Donating data for health and social care research

Many people are willing to contribute to health-related research by actively volunteering to make their personal data available [e.g., from wearable devices, smartphone apps (31)] for specified research purposes where there is expected public benefit [e.g., see (32, 33)]. Examples being the UK Biobank⁷ and Open Humans⁸ [see (8, 15)]. Such data donation activities have also been vital in the response to the COVID-19 pandemic — as illustrated by

⁵ Available at: <https://www.nhs.uk/nhs-app/> (Accessed October 6, 2023).

⁶ Available at: <https://www.uhs.nhs.uk/for-patients/my-medical-record> (Accessed October 6, 2023).

⁷ Available at: <https://www.ukbiobank.ac.uk/> (Accessed October 6, 2023).

⁸ Available at: <https://www.openhumans.org/> (Accessed October 6, 2023).

the many people who voluntarily contributed their data to COVID-19 surveillance research studies [e.g., via the Corona Datenspende App,⁹ DETECT study,¹⁰ Zoe Health Study App¹¹]. People may want to use their personal data stores as a means to donate their personal data from different health networks, apps and devices for use as part of health and social care research.

3.4. Participating in health and social care research

In many cases, there can be limited direct interaction, or absence thereof, between those donating data and researchers in the data analysis process following an act of data donation (34). However, people can participate in research in ways beyond their passive involvement as a data subject (35) — for example, as co-designers or as active non-professional researchers as part of citizen science initiatives [e.g., (36)]. Personal data stores may also offer people the opportunity to “bring your own data” [e.g., (37)], as part of their active participation in health and social care research studies [see (34)] — where it would be considered safe, secure and appropriate [e.g., lawful, ethical] to do so. For instance, seeing that personal data represent a fundamental aspect of personal health technologies [e.g., wearable devices, health apps], such participatory data analysis may help to enrich research studies on usability testing of such technologies [e.g., (38)]. It may also help with patient and public involvement [e.g., see (39)] related to the use of advanced analytics in health — e.g., machine learning models for glucose prediction in real-time could be explained to people with type 1 diabetes through an interactive computational notebook, enabling participants and researchers to explore these models together using real-world data as part of co-design sessions [example based on: (40)].

⁹ Available at: <https://corona-datenspende.de/science/en/> (Accessed October 6, 2023).

¹⁰ Available at: <https://detectstudy.org/> (Accessed October 6, 2023).

¹¹ Available at: <https://health-study.zoe.com/data> (Accessed October 6, 2023).

4. Challenges of developing personal data store ecosystems

To establish the trustworthy personal data store ecosystems that can serve the needs and interests of a wide range of stakeholders in health and social care — e.g., patients, clinicians, researchers — various challenges will need to be resolved [e.g., see (18, 41, 42)]. In this paper, we place particular emphasis on the following four areas of research and implementation challenges:

- People being able to **self-manage** their personal data safely, securely, and appropriately.
- Service providers developing solutions in accordance with **privacy-by-design**.
- All stakeholders committing to the **data work** needed to extract value from data.
- Stakeholders being able to work together to establish the **sustainable infrastructure** necessary for supporting and governing such ecosystems.

4.1. Challenge of self-managing data

Much has been written about the various issues surrounding the notion of self-managing personal data where individuals consent to secondary uses of their data [e.g., see (43, 44, 45, 46, 47)]. For instance, one issue is that while many people often want more control over their personal data, in practice the majority of people do not read privacy notices — or when they do, may not have enough further information and knowledge to make informed decisions over personal data (46). It should also be highlighted that people may not always follow best practices for cybersecurity [e.g., see (48)]. Another issue is that personal data often conveys information about our interactions or relationships with one or more other people (44, 49, 50), decisions to self-manage and share personal data therefore often pose privacy and security risks not only to the personal data store user, but also to those people that they are associated with.

Usage of personal data should also be considered in the context of the existing health app-centric ecosystem — where individuals are often not only motivated to generate and collect progressively more and diverse types of (sensitive) personal data but are also encouraged to share their data with peers and other third parties [e.g., (1, 51)]. In some cases, this may be problematic as individuals may be making available excessive amounts of data about themselves (and others) either intentionally or inadvertently, which may give rise to increased privacy and security risks. As data-rich environments offering people access to extensive archives of personal data (e.g., from multiple health networks, apps, and devices), thought needs to be given to the impact personal data store usage could have on such possible excessive data sharing.

Of course, in some cases, people will not be in the position to self-manage their personal data, or do not want the responsibility of doing so (52). Consideration also must be given to those situations where personal data store ecosystems may have adverse implications for stakeholders, such as where their application in specific contexts would be regarded as: unduly burdensome e.g., self-managing data seen as contributing to “illness work” by patients [e.g., (53)]; inappropriate e.g., as part of participatory research analysis due to ethical

sensitivities; or would contribute to, or otherwise expand, existing health inequalities and digital exclusion (52).

4.2. Challenge of privacy-by-design

The ability of people to self-manage their personal data safely, securely, and appropriately, and their willingness to self-manage data, together pose a significant challenge to the development of personal data store ecosystems (18). While there is no simple solution to addressing such issues, service providers need to develop solutions in accordance with privacy-by-design [see (54)], ensuring that effective mechanisms are in place that can keep data safe and secure by default in multi-stakeholder personal data store ecosystems — and individuals and other stakeholders are supported and encouraged to comply with best practices for privacy, data protection and security across the data lifecycle [e.g., see (48, 55)]. For instance, there needs to be “transparency measures” (24) in place that help people make informed and appropriate decisions about their data [e.g., through standardised “machine-readable policies” (24)], and related assurance measures to demonstrate that once personal data has been shared with others it is used in a manner that they perceive as trustworthy and acceptable [e.g., (56, 57)].

4.3. Challenge of work needed to extract value from data

A considerable amount of time and effort is likely to be required to carry out the various forms of “data work” [see (58, 59)] necessary to make data accumulated in personal data stores meaningful and useful for individuals and other users [e.g., in terms of wellbeing, individual care, research]. Self-management of personal data is one essential component of overall data work required — however, other important functions carried out by service providers adding value to data must also be recognised (22). It should further be noted that by identifying the various forms of data work involved, a better understanding of where such activities may have adverse implications for stakeholders and what measures can be taken to improve the given situation can be achieved.

4.4. Challenge of establishing sustainable infrastructure

Establishing the socio-technical infrastructure necessary to effectively govern, operate, and support the use of multi-stakeholder personal data ecosystems in health and social care will be challenging [e.g., (17, 22, 41, 42)]. For instance, such infrastructure needs to enable data portability between multiple personal data store providers as well as other service providers (e.g., as individuals may decide to switch provider), and interoperability to deliver the services required to support the different uses of personal data stores in health and social care. Further, such infrastructure should facilitate “participatory data stewardship” (15) not only on the account of individuals self-managing their data as part of personal data stores, but also by mechanisms that allow individuals to influence and contribute to how data are governed once made available to others [e.g., for individual care, research] in different “data governance spaces” (60). As personal data stores ecosystems need to appropriately balance risks and benefits at both “individual” and “population” levels (61), attention needs to be given on the types of trusted third-party intermediaries (61) that are required to give rise to robust data

stewardship practices across multi-stakeholder ecosystems — e.g., “consent intermediaries” (44) [for further examples also see (56, 62, 63)].

To establish the necessary infrastructure, there needs to be focus on “whole systems” (30) as well as support and participation from a wide range of stakeholders. However, efforts are being made to move towards such infrastructure e.g., with the proposed development of the European Health Data Space as well as the focus on smart data initiatives (28) and deployment of personal data stores in other domains [e.g., (42)].

Preprint

5. Conclusion

Against the backdrop of progressive digitalisation and datafication of health, we have specifically focused on the development of trustworthy personal data store ecosystems — as one type of socio-technical innovation — providing a person-centred approach that could help to improve the use of data for well-being, individual care and research. As we have highlighted, various opportunities for using personal data stores exist in health and social care, such as for enabling individuals to make better use of their data within health and well-being apps, use data for individual care, donate data, and participate in health and social care research. Yet, developing the trustworthy personal data ecosystems required to support such beneficial uses arising through these different types of stakeholder interactions will be challenging. In this paper, we have placed particular emphasis on four such areas of research and implementation challenges — related to the ability and willingness of individuals to self-manage their data; ensuring privacy-by-design-and-by-default; committing to required data work; and establishing sustainable infrastructure. What is clear from this discussion on motivations, opportunities and challenges is that the development of trustworthy personal data store ecosystems in health and social care calls for a deep understanding of the human factors involved.

Authors contributions

LC: Conceptualisation; Writing — original draft; Writing — review and editing. WH: Conceptualisation; Funding acquisition; Writing — review and editing. MB: Conceptualisation; Funding acquisition; Supervision; Writing — review and editing.

Funding

This study was partly funded by the NIHR Southampton Biomedical Research Centre (NIHR203319) as part of the Data, Health and Society theme.

The views expressed are those of the authors and not necessarily those of the National Institute for Health and Care Research (NIHR) or the Department of Health and Social Care.

Acknowledgements

We would like to thank Dr Lisa Ballard, Prof Age Chapman, Dr Chris Duckworth, Dr Brian Pickering, Dr Paul Smart and Dr Steve Taylor for related discussions about personal data store ecosystems.

LC presented a brief overview of this work at the NIHR Southampton Biomedical Research Centre Open Day, which took place on 9 October 2023.

It should also be noted that MB is the Lead Contact for the COdesigning Trustworthy Autonomous Diabetes Systems [COTADs] project funded by the UKRI Trustworthy Autonomous Systems [TAS] Hub [<https://tas.ac.uk/current-research-projects/cotads/> (Accessed October 16, 2023)] — a project which provided inspiration for an example given in section 3.4 of this paper [see (40)].

Again, please note that all views expressed in this paper are those of the authors and do not necessarily represent those named above.

References

1. **Lalji N.** Featurization and the myth of data empowerment. *Wash JL Tech & Arts.* (2019) 15(1):1-35. Available at: <https://digitalcommons.law.uw.edu/wjlt/vol15/iss1/2> (Accessed October 16, 2023).
2. **Shilton K.** Participatory personal data: An emerging research challenge for the information sciences. *J Am Soc Inf Sci Tec.* (2012) 63(10):1905-1915. doi: 10.1002/asi.22655
3. **Lupton D.** Self-tracking, health and medicine [editorial]. *Health Sociology Review.* (2017) 26(1):1-5. doi: 10.1080/14461242.2016.1228149
4. **Richardson S.** The new physicality of data. *Business Information Review.* (2021) 38(2):67-74. doi: 10.1177/02663821211020194
5. **World Economic Forum (WEF).** *Unlocking the Value of Personal Data: From Collection to Usage* [report]. Industry Agenda prepared in collaboration with The Boston Consulting Group. (2013). Available at: <https://www.weforum.org/reports/unlocking-value-personal-data-collection-usage/> (Accessed October 16, 2023).
6. **Castle-Clark S.** NHS at 70: What will new technology mean for the NHS and its patients? Four big technological trends [briefing]. The Health Foundation, the Institute for Fiscal Studies, The King's Fund and the Nuffield Trust. (2018). Available at: <https://www.health.org.uk/publications/nhs-at-70-what-will-new-technology-mean-for-the-nhs-and-its-patients> (Accessed October 16, 2023).
7. **Brinson, NH, Rutherford, DN.** Privacy and the quantified self: A review of U.S. health information policy limitations related to wearable technologies. *J Consum Aff.* (2020) 54(4):1355-1374. doi: 10.1111/joca.12320
8. **Kariotis T, Ball M, Greshake Tzovaras B, Dennis S, Sahama T, Johnston C et al.** Emerging health data platforms: From individual control to collective data governance. *Data & Policy.* (2020) 2:E13. doi: 10.1017/dap.2020.14
9. **European Commission.** Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation [communication]. Communication from the Commission to the European Parliament and the Council; COM(2020) 264 final. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0264&from=EN> (Accessed October 16, 2023).
10. **Reus J, Bilderbeek N.** Data portability in the EU: An obscure data subject right. IAPP [International Association of Privacy Professionals]: Privacy Perspectives. (March 24, 2022). Available at: <https://iapp.org/news/a/data-portability-in-the-eu-an-obscure-data-subject-right/> (Accessed October 3, 2023).
11. **Sharon T, Lucivero F.** Introduction to the Special Theme: The expansion of the health data ecosystem – Rethinking data ethics and governance [editorial]. *Big Data & Society.* (2019) 6(2). doi: 10.1177/2053951719852969
12. **Ada Lovelace Institute.** The data will see you now: Datafication and the boundaries of health [report]. (2020). Available at: <https://www.adalovelaceinstitute.org/wp-content/uploads/2020/11/The-data-will-see-you-now-Ada-Lovelace-Institute-Oct-2020.pdf> (Accessed October 16, 2023).
13. **Boyd M, Zimeta M, Tennison J, Alassow M.** Secondary use of health data in Europe [report]. Open Data Institute (ODI) — report commissioned by Roche. (2021). Available at: <https://theodi.org/insights/projects/discover-how-ready-your-country-is-for-the-secondary-use-of-health-data/> (Accessed October 16, 2023).
14. **Department of Health and Social Care [UK].** Data saves lives: reshaping health and social care with data [policy paper]. (2022). Available at: <https://www.gov.uk/government/publications/data-saves-lives-reshaping-health-and-social-care-with-data/data-saves-lives-reshaping-health-and-social-care-with-data> (Accessed October 16, 2023).
15. **Ada Lovelace Institute.** Participatory data stewardship: A framework for involving people in the use of data [report]. (2021). Available at: <https://www.adalovelaceinstitute.org/report/participatory-data-stewardship/> (Accessed October 16, 2023).
16. **The Royal Society.** Protecting privacy in practice: The current use, development and limits of Privacy Enhancing Technologies in data analysis [report]. (2019). ISBN: 978-1-78252-390-1. Available at:

https://royalsociety.org/topics-policy/projects/privacy-enhancing-technologies/ (Accessed October 16, 2023).

17. **Janssen H, Cobbe J, Norval C, Singh J.** Decentralized data processing: personal data stores and the GDPR. *International Data Privacy Law*. (2020) 10(4):356–384. doi: 10.1093/idpl/ipaa016
18. **Van Kleek M, O’Hara K.** The Future of Social is Personal: The Potential of the Personal Data Store. In: Miorandi D, Maltese V, Rovatsos M, Nijholt A, Stewart J., editors. *Social Collective Intelligence. Computational Social Sciences*. Springer, Cham. (2014). doi: 10.1007/978-3-319-08681-1_7
19. **Coll L.** Personal data empowerment: Time for a Fairer Deal [report]? The National Association of Citizens Advice Bureaux. (2015). Available at: <https://www.citizensadvice.org.uk/Global/Public/Corporate%20content/Publications/Personal%20data%20empowerment%20report.pdf> (Accessed October 16, 2023).
20. **Carpentier CL.** [with contributions from Cheng HWJ, Jackobs A, Roehrl, R; and inputs from external partners Klauer P, Doerfler K.] New Economics for Sustainable Development: Attention Economy [brief]. United Nations Economist Network. (2023). Available at: https://www.un.org/sites/un2.un.org/files/attention_economy_feb.pdf (Accessed October 16, 2023).
21. **Poikola A, Kuikkanen K, Kuittinen O, Honko H, Knuutila A, Lähteenaja V. (Open Knowledge Finland).** MyData – an introduction to human-centric use of personal data [report]. Third, updated, revised and translated English edition. Lähteenaja V. editor. (MyData Global). Publisher: Ministry of Transport and Communications, Finland (2020). ISBN 978-952-243-617-7. Available at: <https://mydata.org/wp-content/uploads/2020/08/mydata-white-paper-english-2020.pdf> (Accessed October 16, 2023).
22. **Ilves LK, Osimo DA.** A Roadmap for a Fair Data Economy [policy brief]. The Lisbon Council & Sitra. (2019). Available at: <https://www.sitra.fi/app/uploads/2019/04/a-roadmap-for-a-fair-data-economy.pdf> (Accessed October 16, 2023).
23. **Micheli M, Ponti M, Craglia M, Berti Suman A.** Emerging models of data governance in the age of datafication. *Big Data & Society*. (2020) 7(2). doi: 10.1177/2053951720948087
24. **Asgarinia H, Chomczyk Penedo A, Esteves B, Lewis D.** Who Should I Trust with My Data? Ethical and Legal Challenges for Innovation in New Decentralized Data Management Technologies. *Information*. (2023) 14(7):351. doi: 10.3390/info14070351
25. **European Data Protection Supervisor.** Opinion 4/2015 — Towards a new digital ethics: Data, dignity and technology [opinion]. (2015). Available at: https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf (Accessed October 16, 2023).
26. **Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space.** Document 52022PC0197; COM/2022/197 final. (2022). Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0197> (Accessed October 16, 2023).
27. **European Parliament.** European health data space [briefing]. (2022). EU Legislation in Progress. Available at: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733646/EPRS_BRI\(2022\)733646_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733646/EPRS_BRI(2022)733646_EN.pdf) (Accessed October 16, 2023).
28. **Challenge Works [a Nesta Enterprise], DeepSeer.** Unlocking Smart Data: Design Research into a Possible Smart Data Challenge Prize [report]. (2023). Research conducted on behalf of the Department for Business and Trade (UK). Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1168934/smart-data-challenge-prize-final-report.pdf (Accessed October 16, 2023).
29. **Estrada-Galíñanes V, Wac K.** Collecting, Exploring and Sharing Personal Data: Why, How and Where. *Data Science*. (2020) 3(2):79–106. doi: 10.3233/DS-190025
30. **Chute C, French T, Raman S, Bradley J.** User Requirements for Comanaged Digital Health and Care: Review. *J Med Internet Res*. (2022) 24(6):e35337. PMID: 35687379. PMCID: 9233266. doi: 10.2196/35337
31. **Amft O, Lopera González LI, Lukowicz P, Bian S, Burggraf, P.** Wearables to Fight COVID-19: From Symptom Tracking to Contact Tracing. *IEEE Pervasive Computing*. (2020) 19(4):53-60. doi: 10.1109/MPRV.2020.3021321

32. **Baara M, Lipset C, Kudumala Fox J, Israel, A.** Blockchain opportunities for patient data donation & clinical research. Deloitte Consulting LLP & Pfizer. (2018). Available at: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/process-and-operations/us-cons-blockchain-opportunities-patient-data-donation-clinical-research.pdf> (Accessed October 16, 2023).
33. **Skatova A, Goulding J.** Psychology of personal data donation. *PLoS ONE*. (2019) 14(11): e0224240. doi: 10.1371/journal.pone.0224240
34. **Gomez Ortega A, Bourgeois J, Kortuem G.** Reconstructing Intimate Contexts through Data Donation: A Case Study in Menstrual Tracking Technologies. (2022). In *Nordic Human-Computer Interaction Conference (NordiCHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 8, 1–12. doi: 10.1145/3546155.3546646
35. **Smits DW, van Meeteren, K, Klem M, Alsem M, Ketelaar M.** Designing a tool to support patient and public involvement in research projects: the Involvement Matrix. *Research Involvement and Engagement*. (2020) 6, 30. doi: 10.1186/s40900-020-00188-4
36. **Borda A, Gray K, Fu Y.** Research data management in health and biomedical citizen science: practices and prospects. *JAMIA Open*. (2020) 3(1):113–125. doi: 10.1093/jamiaopen/ooz052
37. **Meurisch C, Bayrak B, Muhlhäuser M.** EdgeBox: Confidential Ad-Hoc Personalization of Nearby IoT Applications. *IEEE Global Communications Conference (GLOBECOM)*. (2019) 1–6. doi: 10.1109/GLOBECOM38437.2019.9013520
38. **Zazelenchuk T, Sortland K, Genov A, Sazegari S, Keavney M.** Using participants' real data in usability testing: lessons learned. In *CHI '08 Extended Abstracts on Human Factors in Computing Systems (CHI EA '08)*. Association for Computing Machinery (ACM), New York, NY, USA. (2008) 2229–2236. doi: 10.1145/1358628.1358656
39. **Zidaru T, Morrow EM, Stockley R.** Ensuring patient and public involvement in the transition to AI-assisted mental health care: A systematic scoping review and agenda for design justice. *Health Expectations*. (2021) 24(4):1072–1124. doi: 10.1111/hex.13299
40. **Ayobi A, Hughes J, Duckworth C, Dylag J, James S, Marshall P et al.** Computational Notebooks as Co-Design Tools: Engaging Young Adults Living with Diabetes, Family Carers, and Clinicians with Machine Learning Models. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23)* (Vol. 2023). Association for Computing Machinery (ACM). doi: 10.1145/3544548.3581424
41. **Brochot G, Brunini J, Eisma F, Larsen R, Lewis DJ, Zhang J [Academic Supervisor].** Report on Personal Data Stores for the European Commission [report]. Judge Business School, University of Cambridge; Commissioned by DG Connect. (2015). Available at: <https://wayback.archive-it.org/12090/20160322175905/https://ec.europa.eu/digital-single-market/en/news/study-personal-data-stores-conducted-cambridge-university-judge-business-school> (Accessed October 16, 2023).
42. **Van Damme S, Merchant P, Vlassenroot E, Van Compernolle M, Buyle R, Bauwens D.** Towards a Research Agenda for Personal Data Spaces: Synthesis of a Community Driven Process. In: Janssen M et al. *Electronic Government. EGOV 2022*. Lecture Notes in Computer Science, vol 13391. Springer, Cham (2022). doi: 10.1007/978-3-031-15086-9_36
43. **Lazaro C, Le Métayer D.** Control over Personal Data: True Remedy or Fairy Tale? *SCRIPTed*. (2015) 12:1. doi: 10.2966/scr.120115.3
44. **Lehtiniemi T, Kortesniemi Y.** Can the obstacles to privacy self-management be overcome? Exploring the consent intermediary approach. *Big Data & Society*. (2017) 4(2). doi: 10.1177/2053951717721935
45. **O'Hara K.** Privacy, Privacy-Enhancing Technologies & the Individual [white paper]. Web Science Trust (WST) White Paper #1. (2022). Available at: https://webscience.org/wp-content/uploads/2022/03/Privacy-Individual-Book-Ohara.final_.pdf (Accessed October 16, 2023).
46. **Solove DJ.** Introduction: privacy self-management and the consent dilemma. *Harvard Law Review*. (2013) 126(7):1880–1903. Available at: <https://heinonline.org/> (Accessed October 16, 2023).
47. **Vayena E, Blasimme A.** Biomedical Big Data: New Models of Control Over Access, Use and Governance. *Journal of Bioethical Inquiry*. 2017; 14: 501–513. doi: 10.1007/s11673-017-9809-6
48. **Coventry L, Briggs P, Blythe J, Tran M.** Using behavioural insights to improve the public's use of cyber security best practices [summary report]. (2014). Government Office for Science. Available at:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/309652/14-835-cyber-security-behavioural-insights.pdf (Accessed October 16, 2023).

49. **Harkness T.** The history of the data economy: Part IV: The future. *Significance*. (2021) 18(6):12-15. doi: 10.1111/1740-9713.01586
50. **von Hanxleden R.** Information: 'I' vs. 'we' vs. 'they' [viewpoint]. *Communications of the ACM*. (2022) 65(5):45-47. doi: 10.1145/3491205
51. **Lanzing M.** The transparent self. *Ethics and Information Technology*. (2016) 18: 9–16. doi: 10.1007/s10676-016-9396-y
52. **Pasquale F.** Redescribing Health Privacy: The Importance of Information Policy. *Hous J Health L & Pol'y*. (2014) 14: 95-128. Available at: <https://heinonline.org/> (Accessed October 16, 2023).
53. **Ancker JS, Witteman HO, Hafeez B, Provencher T, Van de Graaf M, Wei E.** "You Get Reminded You're a Sick Person": Personal Data Tracking and Patients With Multiple Chronic Conditions. *J Med Internet Res*. (2015) 17(8): e202. doi: 10.2196/jmir.4209
54. **Cavoukian A.** Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D. *IDIS*. (2010) 3:247–251. doi: 10.1007/s12394-010-0062-y
55. **Stalla-Bourdillon S, Thuemer G, Walker J, Carmichael L, Simperl E.** Data protection by design: Building the foundations of trustworthy data sharing. *Data & Policy*. (2020) 2: E4. doi: 10.1017/dap.2020.1
56. **Boniface M, Carmichael L, Hall W, Pickering B, Stalla-Bourdillon S, Taylor S.** The Social Data Foundation model: Facilitating health and social care transformation through *datatrust services*. *Data & Policy*. 2022; 4: E6. doi: 10.1017/dap.2022.1
57. **Snaith B, Yates D, Evans E.** Assurance, trust, confidence — what does it all mean for data [blog post]? Open Data Institute (ODI) Blog. (2021, June 18). Available at: <https://www.theodi.org/article/assurance-trust-confidence-what-does-it-all-mean-for-data/> (Accessed October 16, 2023).
58. **Fiske A, Prainsack B, Buyx A.** Data Work: Meaning-Making in the Era of Data-Rich Medicine. *J Med Internet Res*. (2019) 21(7):e11672. PMID: 31290397; PMCID: 6647753. doi: 10.2196/11672
59. **Bossen C, Pine KH, Cabitzka F, Ellingsen G, Piras EM.** Data work in healthcare: An introduction. *Health Informatics Journal*. (2019) 25(3):465–474. doi: 10.1177/1460458219864730
60. **Paparova D, Aanestad M, Vassilakopoulou P, Klungland Bahus M.** Data governance spaces: The case of a national digital service for personal health data. *Information and Organization*. (2023) 33(1):100451. ISSN 1471-7727. doi: 10.1016/j.infoandorg.2023.100451
61. **Viljoen S.** A relational theory of data governance. *Yale Law Journal*. (2021) 131(2):573-654. Available at: <https://heinonline.org/> (Accessed October 16, 2023).
62. **Kang J, Shilton K, Estrin D, Burke J.** Self-surveillance privacy. *Iowa Law Review*. (2012) 97(3): 809-848. Available at: <https://heinonline.org/> (Accessed October 16, 2023).
63. **Mechant P, De Wolf R, Van Compernolle M, Joris G, Evens T, De Marez L.** Saving the web by decentralizing data networks? A socio-technical reflection on the promise of decentralization and personal data stores. (2021). *14th CMI International Conference - Critical ICT Infrastructures and Platforms (CMI), 2021*, pp. 1-6. doi: 10.1109/CMI53512.2021.9663788