Data & Policy (2022), 4: e6
doi:10.1017/dap.2022.1

RESEARCH ARTICLE

The Social Data Foundation model: Facilitating health and social care transformation through *datatrust services*

Michael Boniface[1], Laura Carmichael[1,*], Wendy Hall[1], Brian Pickering[1], Sophie Stalla-Bourdillon[2] and Steve Taylor[1]

[1]Electronics & Computer Science, University of Southampton, Southampton, United Kingdom
[2]Law, University of Southampton, Southampton, United Kingdom
*Corresponding author. E-mail: L.E.Carmichael@soton.ac.uk

Received: 16 June 2021; **Revised:** 17 December 2021; **Accepted:** 10 January 2022

Key words: data governance models; data institutions; data stewardship; *datatrust* services; healthcare and social care

Abbreviations: AI, artificial intelligence; API, application programming interface; CHIA, Care and Health Information Exchange Analytics; DARS, Data Access Request Service; DLT, distributed ledger technology; DPIA, data protection impact assessment; DPO, data protection officer; DSAP, data sharing and analysis project; GDPR, General Data Protection Regulation; HL7 FHIR, Health Level 7 Fast Healthcare Interoperability Resources; HRA, Health Research Authority; ICO, Information Commissioner's Office; ICS, integrated care system; ISO, International Organization for Standardization; MELD, Multidisciplinary Ecosystem to study Lifecourse Determinants of Complex Mid-life Multimorbidity using Artificial Intelligence; ML, machine learning; MLTC-M, multiple long term conditions—multimorbidity; NHS, National Health Service (UK); NHS REC, NHS Research Ethics Committee; NIHR, National Institute for Health Research (UK); ONS, Office for National Statistics; OWASP, Open Web Application Security Project; PETs, privacy enhancing-technologies; PI, principal investigator; RDA, Research Data Alliance; SDF, Social Data Foundation; SD-WANS, software-defined wide area networks; TRE, trusted research environment; UK, United Kingdom; UKDS, UK Data Service; UKHDRA, UK Health Data Research Alliance; WSI, Web Science Institute

Abstract

Turning the wealth of health and social data into insights to promote better public health, while enabling more effective personalized care, is critically important for society. In particular, social determinants of health have a significant impact on individual health, well-being, and inequalities in health. However, concerns around accessing and processing such sensitive data, and linking different datasets, involve significant challenges, not least to demonstrate trustworthiness to all stakeholders. Emerging *datatrust services* provide an opportunity to address key barriers to health and social care data linkage schemes, specifically a loss of control experienced by data providers, including the difficulty to maintain a remote reidentification risk over time, and the challenge of establishing and maintaining a social license. *Datatrust services* are a sociotechnical evolution that advances databases and data management systems, and brings together stakeholder-sensitive data governance mechanisms with data services to create a trusted research environment. In this article, we explore the requirements for *datatrust services*, a proposed implementation—the Social Data Foundation, and an illustrative test case. Moving forward, such an approach would help incentivize, accelerate, and join up the sharing of regulated data, and the use of generated outputs safely amongst stakeholders, including healthcare providers, social care providers, researchers, public health authorities, and citizens.

Policy Significance Statement

Turning the wealth of health and social data into insights for better public health and personalized care is critically important for society. Yet data access and insights are hampered by manual governance processes that can be time consuming, error-prone, and not easy to repeat. With increasing data volumes, complexity, and need for ever-faster

https://doi.org/10.1017/dap.2022.1 Published online by Cambridge University Press

solutions, new approaches to data governance must be found that are secure, rights-respecting, and endorsed by communities. The Social Data Foundation combines governance with *datatrust services* to allow citizens, service providers, and researchers to work together to transform systems. By bridging the gap between data and trust services, new progressive models of data governance can be established offering high levels of data stewardship and citizen participation.

1. Introduction

Social determinants of health significantly affect individual well-being and health inequalities (Sadana and Harper, 2011; Public Health England, 2017; Marmot et al., 2020). The World Health Organization (n.d.) describes "social determinants of health" as "nonmedical factors that influence health outcomes" such as "education," "working life conditions," "early childhood development," and "social-inclusion and nondiscrimination." The global COVID-19 pandemic highlights how "disparities in social determinants of health" (Burström and Tao, 2020) give rise to poorer health outcomes for some groups in society. For instance, disadvantaged economic groups appear to be at greater risk of exposure to COVID-19, and are more susceptible to severe disease or death (e.g., Abrams and Szefler, 2020; Burström and Tao, 2020; Triggle, 2021).

Social determinants of health can be acquired from diverse data sources—for example, wearables, digital health platforms, social media, and environment monitoring—many beyond the conventional boundaries of health and social care (e.g., Sharon and Lucivero, 2019). The "safe" linkage (UK Data Service, n.d.; UK Health Data Research Alliance, 2020) of good quality data is therefore vital for the generation of insights supporting positive health and social care transformation.[1] Specifically, newer forms of social determinants of health data (e.g., from wearables) need to bring together with other more conventional data types (e.g., electronic healthcare records, public health statistics, and birth cohorts datasets) for analysis by multidisciplinary researchers and practitioners, including the application and development of new and existing health data science methods and tools. Such data-driven insights can be used to "improve decision-making at the individual and community level" (Galea et al., 2020) thus promoting better public health,[2] enabling more effective personalized care,[3] and ultimately helping address inequalities in health.

Although the need for sustainable and positive health and social care transformation is widely accepted in principle, more needs to be done in practice to derive benefit from available data. This includes incentivizing and accelerating sharing of regulated data and any associated outputs across relevant stakeholders (e.g., healthcare or social care providers, researchers, public health authorities, and citizens). Many health and social care datasets remain in silos under the control of individual groups or institutions (Kariotis et al., 2020), giving rise to data monopolies or oligopolies. Slow, disjointed, manual governance processes—often error-prone, time consuming, and difficult to repeat—hamper data access and insights.[4] This has been accentuated by the extraordinary situation of the global COVID-19 pandemic (e.g., Research Data Alliance (RDA) COVID-19 Working Group, 2020). Trustworthy data governance is essential not only to ensure data providers and data users can fulfill their regulatory obligations, but also to maintain public confidence and engagement (Geissbuhler et al., 2013; Stalla-Bourdillon et al., 2021).

[1] Note that a key theme for positive health and social care transformation is the design and implementation of "integrated care systems" (ICSs) for seamless care delivery across the health and social care pathways (NHS, 2019)—also referred to as "hospitals without walls" (Hawkes, 2013; Spinney, 2021).

[2] For example, via public interventions, targeted health, and well-being campaigns.

[3] For example, through personalized medicine, increased patient and/or service user empowerment, and better operational efficiency for health and care service providers.

[4] In the UK, the NHS remains a key provider of clinical and administrative data for research and innovation (i.e., secondary use of data for nonclinical purposes) related to health and social care systems transformation. Data users can request access to data, for example, via applications to Data Access Request Service (DARS) (NHS Digital, n.d.) provided by NHS Digital, individual NHS trusts and foundations, and local health and care records programmes (e.g., Wessex Care Records (2021)).

https://doi.org/10.1017/dap.2022.1 Published online by Cambridge University Press

Advanced data governance[5] models are therefore required that can foster a "social license" (Carter et al., 2015; Jones and Ford, 2018; O'Hara, 2019) and which can handle increasing data volumes and complexity safely (e.g., Sohail et al., 2018; Winter and Davidson, 2019).

To enable fast, collaborative, and trustworthy data sharing that meets these needs, we propose a Social Data Foundation for Health and Social Care ("the SDF") (Boniface et al., 2020), as a new form of data institution.[6] Based on the "Five Safes Plus One," and the concept of the "trusted research environment (TRE)" (The UK Health Data Research Alliance, 2020), the SDF proposes *datatrust services* as a sociotechnical model for good data governance, sensitive to the needs of all stakeholders, and allied with advances in dynamic and secure federated research environments.

This article considers how health and social care transformation can be facilitated through *datatrust services*—and is divided into four main parts.[7] First, in Section 2, we explore the conceptual basis for TREs within the health and social care domain. Second, in Section 3, we demonstrate why the SDF model is well equipped to support health and social care transformation for individual and community benefit,[8] boost open science, and generate insights for multiple stakeholders—by providing an overview of the SDF governance structure and an implementation of *datatrust services.* Third, in Section 4, we validate our SDF model through its application to a test case centered on social determinants of health research: the "Multidisciplinary Ecosystem to study Lifecourse Determinants of Complex Mid-life Multimorbidity using Artificial Intelligence" (MELD) project (MELD, 2021). Finally, in Section 5, we summarize the key points raised and outline next steps for the SDF model.

2. "TREs" in Health and Social Care: Motivation and Key Requirements

Best practice for health and social care research and innovation—specified by the UK Health Data Research Alliance (UKHDRA) (2020)—necessitates that data sharing and linkage occurs within TREs, providing:

> a secure space for researchers to access sensitive data. Commonly referred to as 'data safe havens,' TREs are based on the idea that researchers should access and use data within a single secure environment (Harrison, 2020).

This section examines the concept of a "TRE" when used for linking data held by different parties for the purpose of health and social care transformation.

2.1. Challenges with the "data release model"

Despite the long-established notion of the "data safe haven" (Burton et al., 2015),[9] health and social data linkage typically uses a "data release model": data are made available to approved users in their own data environments (UKHDRA, 2020).

[5] While there is no universal definition of the term "data governance," Janssen et al. (2020) provide a useful description of this term in a multiorganizational context: "Organizations and their personnel defining, applying, and monitoring the patterns of rules and authorities for directing the proper functioning of, and ensuring the accountability for, the entire life-cycle of data and algorithms within and across organizations." Note that Smart Dubai and Nesta (2020) describe collaborative data governance innovation as "fairly embryonic" in practice.

[6] The phrase "data institution" is used by the Open Data Institute (ODI) as an umbrella term to describe: "organizations whose purpose involves stewarding data on behalf of others, often towards public, educational or charitable aims" (Dodds et al., 2020).

[7] A glossary of key terms is provided after the main text of this article.

[8] For example, alignment with the CARE principles (2018).

[9] Trusted third party intermediaries continue to play a crucial role in facilitating data linkage for public health research and innovation—such as, SAIL (2021; Jones et al., 2014) for linkage of specified anonymized datasets, and UKHDRA (n.d.) for discoverability of particular UK health datasets held by members through its Innovation Gateway. For further discussion of this point, the Public Health Research Data Forum (2015) provides 11 case studies of data linkage projects from across the world, and outlines barriers and key lessons to be learnt. For further examples of health data sharing initiatives also see: ICES, Canada (2021); and Data Linkage Western Australia (2021).

https://doi.org/10.1017/dap.2022.1 Published online by Cambridge University Press

The data release model can be problematic. Firstly, health and social care data are often rich and large-scale requiring “diverse tooling” (UKHDRA, 2020). However, data safe havens were “until recently” only able to provide limited tools for data analysis (UKHDRA, 2020) as well as “secure remote working solutions, real-time anonymisation, and synthetic data” (Desai et al., 2016). Further, once data are shared, data providers often experience a loss of control over their data. They have reduced oversight over how data are accessed, linked, and reused. Generated outputs from any data linkage activities (e.g., containers, derived data, images, notebooks, publications, and software) are often not adequately disclosed (UKHDRA, 2020), making it more difficult to effectively mitigate the risk of reidentification, and increasing potential “mosaic effects” (Pozen, 2005).

In some cases, this loss of control and visibility may act as disincentives to sharing data with higher levels of utility[10] (e.g., data providers may share only aggregated data where deidentified data at the individual level may offer greater societal benefit), or sharing any data whatsoever. A lack of control, transparency, and measurement of benefit may also prevent, weaken, or nullify a social license (defined below) for specific health and social care research and innovation activities.

2.2. Upholding a social license

Fulfilling legal obligations alone is not enough to secure social legitimacy for health and social care research and innovation (Carter et al., 2015)—TREs require a “social license” defined by Muller et al. (2021) as follows:

> A social licence in the context of data-intensive health research refers to the non-tangible societal permission or approval that is granted to either public or private researchers and research organisations. This allows them to collect, use, and share health data for the purpose of health research by virtue of those activities being trustworthy, by which is meant trusted to be in line with the values and expectations of the data subject communities, stakeholders, and the public.

A social license, therefore, is dependent on perceptions by the main stakeholders that what is being done is acceptable and beneficial (Rooney et al., 2014). Applied to the TRE, its social license is supported by its perceived trustworthiness (which can be expressed in terms of benevolence, integrity, and ability [Mayer et al., 1995]) toward the communities it intends to serve. For instance, aligning ethical oversight with the CARE Principles for Indigenous Data Governance (2018)—that is, “collective benefit,” “authority to control,” “responsibility,” and “ethics”—brings to center stage the need to ensure equanimity across the data lifecycle. The UKHDRA (2020) describes the principal rationale for TREs as follows:

> [to] protect—by design—the privacy of individuals whose health data they hold, while facilitating large scale data analysis using High Performance Computing that increases understanding of disease and improvements in health and care.

Along similar lines, the Research Data Alliance (RDA) outlines TRUST principles for data infrastructures—that is, “Transparency,” “Responsibility,” “User Focus,” “Sustainability,” and “Technology” (Lin et al., 2020). However, changes in technology, especially within data science, introduce other issues. Given the availability of ever-increasing volumes of people-centric data, the Toronto Declaration (2018) highlights the fundamental human rights of data subjects, especially for those felt to be particularly

[10] While strong deidentification of data is vital to protect the rights of (groups of) individuals, deidentification can lower the utility of data. The definition of anonymized data is provided by GDPR (2016) Recital 26, namely “information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.” Although strictly speaking, Recital 26 is not binding it has been used by the Court of Justice of the European Union and other national courts to interpret the concept of anonymized data. As a matter of principle, two different processes can lead to anonymized data: a risk-based approach to aggregation (i.e., data is aggregated, e.g., to produce counts, average sums) or a risk-based approach to deidentification (i.e., data remains at the individual-level). In both cases, data and context controls should be combined to guarantee that reidentification risk is “remote” over time (ICO, 2012).

https://doi.org/10.1017/dap.2022.1 Published online by Cambridge University Press

vulnerable. Similarly, the UK Data Ethics Framework (Central Digital and Data Office, 2020) champions the overarching principles of transparency, accountability, and fairness. As well as compliance with relevant law and constant review of individual rights, the framework seeks to balance community needs against those rights. Governance must include all relevant, possibly cross-disciplinary expertise, and ongoing training, of course. In a similar vein with artificial intelligence (AI) technologies, the European Commission (2019) and the UK Department of Health and Social Care (2021) both emphasize respect for individual rights within the context of potential community benefit, accountability, and transparency. Beyond this, though, for stakeholders to agree on a social license, it must be clear that the rights and expectations of individuals and the communities they represent should be upheld.

2.3. Bringing citizens back to center stage

To promote social license and public trust, collaborative data-sharing initiatives need to (re)connect data citizens with data about them and its utility. This is particularly pertinent as health and social care research and innovation becomes increasingly data-driven (Aitken et al., 2020) with national and international data aggregators aiming to increase the power of AI through collection of ever-larger population and disease-specific datasets. In such circumstances provenance, transparency of (re)use, and benefits suffer the risk of opacity; citizen inclusion must be embedded in the design and operation of such processes.

Further, the secondary use of data continues to increase (Jones and Ford, 2018), yet is often less understood by citizens (CurvedThinking, 2019). While such citizen engagement and participation is not new within the health and social care domain, more needs to be done to empower citizens and ensure greater inclusivity in practice (Ocloo and Matthews, 2016)—especially where healthcare data are (re)used by third parties (Understanding Patient Data and Ada Lovelace Institute, 2020). Precedence must be given to meaningful citizen engagement and participation (Davidson et al., 2013; Ford et al., 2019), which remain “inclusive and accessible to broad publics” (Aitken et al., 2020). Of course, given citizens are the focus of public health promotion, recipients of care, and data subjects, it is important they not only have access to information about how data are being (re)used, but also have a voice in the transformation of health and social care systems.

In a world of data-driven policies and technologies, citizen voice and agency will increasingly be determined by participation in datasets themselves. Unless minority representation in datasets is addressed, bias and health inequalities will continue to be propagated. As such, citizen engagement, participation, and empowerment should be viewed as core to health and social care data governance (e.g., Hripcsak et al., 2014; Miller et al., 2018). In particular, there needs to be inclusion of appropriately representative citizens—along with other stakeholders—in the codesign and coevaluation of digital health and social care solutions—to ensure that the benefits derived from “safe outputs” are “measured and evidenced” (Centre for Data Ethics and Innovation, 2020) for communities and individuals.

2.4. Maintaining cohesion and the “diameter of trust”

Existing data-sharing relationships between stakeholder communities (e.g., a specific university, local council, and hospital) can be replicated and strengthened through a TRE. To maintain the cohesiveness of such a community, extensions to membership and engagement need careful consideration as they relate to notions of community-building around TRE interactions. A “diameter of trust” (Ainsworth and Buchan, 2015; Ford et al., 2019; Northern Health Science Alliance, 2020) provides a means to:

> gauge the size and characteristics of a learning, sustainable and trustworthy system (MedConfidential, 2017).

A diameter of trust may be defined for a data institution by examining:

(i) “The level at which engagement with the citizen can be established […]”
(ii) “The extent of patient flows within the health economy, between organisations […]”
(iii) “The scale of a data platform being of sufficient size to enable effective population analyses […]” and

https://doi.org/10.1017/dap.2022.1 Published online by Cambridge University Press

(iv) "The ability to bring data together from the wider determinants of health and care relevant for that population in near real-time […]" (MedConfidential, 2017).

As such, mechanisms need to be in place for a TRE, therefore, to expand while appreciating potential impacts of community size. A diameter of trust cannot be predicated solely on demographics (e.g., geographic scope and community), and trustworthiness must be demonstrated through the operation of a data institution and its proven outcomes, which will in turn encourage trust responses from its stakeholders (e.g., O'Hara, 2019).

2.5. Progressive governance

To remain effective and appropriate, a data governance model for a TRE must be progressive, learning iteratively, integrating new best practices without undue delay, as well as remaining compliant with the changing legal landscape. Best practice may be both organizational (e.g., the adoption of codes of conduct and ethical frameworks) and technical (e.g., application of advanced security and privacy-enhancing technologies [PETs]) in nature. To maintain trustworthiness, crucially, it must adapt to the experience and concerns of all key stakeholders (data subjects, data providers, service providers, researchers, etc.). For instance, Understanding Patient Data (Banner, 2020) has provided a first iteration of a high-level "learning data governance model" that aims to meaningfully integrate citizen views within the decision-making lifecycle.

Lessons may be learned not only from the day-to-day practicalities of supporting individual research projects, through the outputs of citizen engagement and participation activities, but also externally via authoritative national and international guidance. As Varshney (2020) asserts:

> progressive data governance encourages fluid implementation using scalable tools and programs.

Therefore, progressive data governance is essential, and contingent on greater automation of data governance processes and tooling to accelerate trustworthy and collaborative data linkage (Sohail et al., 2018; Moses and Desai, 2020).

2.6. Adhering to the "Five Safes Plus One"

Best practice for TREs is centered on the "Five Safes Framework" (UKHDRA, 2020). The framework was devised in 2003 for the Office for National Statistics (ONS), and is used "for designing, describing, and evaluating access systems for data" (Desai et al., 2016). An additional safe—"Safe Return"—has been added by UKHDRA (2020), which is described below. The "Five Safes Plus One" approach identifies the key "dimensions" (Arbuckle and Ritchie, 2019) that influence the risk and trustworthiness of health and social care research projects—and are provided as "adjustable controls rather than binary settings" (UKHDRA, 2020).

For our purposes, based on the interpretation of the UKHDRA (2020), the six dimensions are as follows:

- "*Safe people*": only trusted and authorized individuals (e.g., vetted researchers working on ethically approved projects in the interests of the public good) shall have access to the data within the TRE.
- "*Safe projects*": only approved projects shall be carried out via the TRE that are legally and ethically compliant and have "potential public benefit."
- "*Safe setting*": the TRE shall provide a trust-enhancing technical ("safe computing") and organizational infrastructure to ensure all data-related activities are undertaken securely and safely.
- "*Safe data*": all other "safes" are adhered to; data are deidentified appropriately before reusage via the TRE, and remain appropriately deidentified across the life-cycle of an approved project.
- "*Safe outputs*": all outputs generated from data analysis activities, undertaken via the TRE, must not be exported without authorization.

- "*Safe return*": to ensure that recombination of TRE outputs with other data at "the clinical setting that originated the data"—which may reidentify data subjects—is only undertaken if permitted and consented by the data subjects concerned. (UKHDRA, 2020).[11]

A collaborative health and social care data-sharing scheme must also fulfill essential data governance requirements for ethics (e.g., institutional approval, Integrated Research Application System (IRAS) [2021] approval), legal-compliance (e.g., data protection, confidentiality, contracts, and intellectual property), and cyber-security (e.g., UK Cyber Essentials Plus [National Cyber Security Centre, n.d.], ISO27001 [ISO, 2013], NHS Data Security and Protection Toolkit, 2021).[12]

3. The SDF Model

Models of safe and high-quality data linkage from multiple agencies necessitate a high level of interdisciplinarity (Jacobs and Popma, 2019) wider than the conventional boundaries of medicine and social care (Ford et al., 2019; Sharon and Lucivero, 2019). To address this, the SDF model has adopted a sociotechnical approach[13] to governing data (e.g., Young et al., 2019) where the multidisciplinary aspects (including, ethical, healthcare, legal, social care, social–cultural, and technical issues) of safe linkage for health and social care transformation are considered collectively and holistically from the outset.

A key objective of the SDF is to accommodate different stakeholder communities and maintain their approval at a level sufficient for engagement and participation. Since multistakeholder health and social care data needs to be aggregated at various levels (e.g., locally, regionally, and nationally), the SDF offers a localized hub for data-intensive research and innovation facilitating multiparty data sharing through a community of vetted stakeholders—including healthcare providers, social care providers, researchers, and public health authorities. Consequently, stakeholders can work together on projects facilitated by the SDF to discover solutions to health and social care transformation, promote greater collaboration, address key local priorities and rapidly respond to new and emerging health data-related challenges, while offering national exemplars of health system solutions.

In order for the SDF to acquire and maintain a social license, any community and individual benefits arising from the SDF must be "measured and evidenced" (Centre for Data Ethics and Innovation, 2020) as well as potential risks and constraints—and disseminated to communities and stakeholders in a transparent manner.[14] The SDF model therefore includes a standard process to identify, monitor, and measure project outputs for different stakeholders. Metrics here include: the alignment between project strategy and its generated outputs; resource allocation compared with action recommendations from generated project outputs; and, demonstrated positive health and social care transformation impacts for certain stakeholder groups.

While the "Five Safes Plus One" approach provides a useful guide by which to design, describe, and evaluate TREs, it does not specify how to implement governance and technology to enable these six safes. To address this, our SDF model interlinks two key threads: governance and technology. We first describe the SDF governance model, then the SDF *datatrust services* supporting the management of data services through functional anonymization, risk management, ownership/rights management, and audit. A concluding section describes how the combined governance and technical approach addresses the requirements identified in Section 2.

[11] It is worthwhile to note that pursuant to section 171(1) of the Data Protection Act (2018) (UK): "It is an offence for a person knowingly or recklessly to reidentify information that is deidentified personal data without the consent of the controller responsible for deidentifying the personal data."

[12] For a nonexhaustive list of data governance requirements, see Boniface et al. (2020).

[13] Note that the SDF initiative brings together a multidisciplinary team of clinical and social care practitioners with data governance, health data science, and security experts from ethics, law, technology and innovation, web science, and digital health.

[14] As a benchmark for best practice, see the five-point framework for evaluating whether a potential data sharing activity can be considered to be of public benefit outlined by Scott (2018).

https://doi.org/10.1017/dap.2022.1 Published online by Cambridge University Press

3.1. SDF governance

The overall purpose of SDF governance model is to facilitate the safe (re)usage of data through "well-defined data governance roles and processes" that builds "prompt and on-going risk assessment and risk mitigation into the whole data lifecycle" (Stalla-Bourdillon et al., 2019)—ultimately to ensure SDF activities deliver positive health and social care transformation for stakeholders. Effective governance therefore must enable the SDF Platform and its Facilitator (defined below) to exercise best practice and progressive governance in support of "Data Sharing and Analysis Projects" (DSAPs) that are legally compliant, respect ethical considerations, and maintain a social license.

Governance needs to take into account the requirements, sensitivities, and vulnerabilities of stakeholders (especially those of stakeholders who are not directly involved in decision-making), so that SDF governance must adopt the key fiduciary ethical virtues of loyalty and care (O'Hara, 2021).[15] However, the relationship is *not* a fiduciary one in the full *legal* sense,[16] because the purpose of the SDF is not to serve a narrow range of stakeholders' interests exclusively, but to deliver positive outcomes across the full range of stakeholders (including service providers and data controllers themselves) while behaving in a trustworthy manner and retaining trust (O'Hara, 2021). SDF governance is not intended to constrain decision-makers' abilities to make the best decisions for their own organizations, but rather to include, and be seen to include, the full range of relevant legitimate interests (O'Hara, 2019).

3.1.1. SDF governance structure

The SDF Governance model builds on the "Data Foundations Framework" (Stalla-Bourdillon et al., 2019, 2021) developed by the Web Science Institute (WSI) at the University of Southampton (UK) and Lapin Ltd (Jersey). The Data Foundations Framework advocates and provides guidance on robust governance mechanisms for collective-centric decision-making, citizen representation, and data stewardship, so is a suitable basis for the SDF Governance, whose structure is shown in Figure 1.

The main bodies, roles, and stakeholders that form the "SDF Governance Structure" are as follows:

- *Advisory Committee*: A group of individuals external to the SDF—with a wide range of expertise related to health and social care transformation (e.g., health and social care services, cyber-security, data governance, health data science, ethics, and law)—that provides advice to the SDF Board on matters related to data sharing (as necessary).
- *Citizen Representatives*: Experts in patient/service user voice, who are mandatory members of the SDF Board (see below), and oversee the administration of citizen participation and engagement activities to ensure that the SDF maintains a social license. In particular, Citizen Representatives shall create, implement and manage a framework for citizen participation and engagement activities, where citizens can cocreate and participate in health and social care systems transformation as well as exercise their data-related rights.[17]
- *Data Provider*: An entity is the owner or rights holder of data that is either discoverable via the Platform, hosted by the Platform, or utilized in DSAPs. The Data Provider is typically an organizational role, represented by a senior person, who has authority to share the data. A representative of a Data Provider could act as a member of the SDF Board.
- *Data User*: An entity that discovers, uses, and/or reuses shared data made accessible via the SDF, or manages DSAPs that are facilitated by the SDF Platform. The Data User role is subdivided into:

[15] The authors are grateful for discussions with Prof. Kieron O'Hara on an earlier version of this article—specifically on the notion of fiduciary ethical virtues in relation to *datatrust services*.

[16] For instance, in the legal sense a fiduciary is "[a] person to whom power or property is entrusted for the benefit of another"—where "[d]uties [are] owed by a fiduciary to a beneficiary"—for example, "a duty of confidentiality," "a duty of no conflict," and "a duty not to profit from his position" (Thompson Reuters: Practical law, n.d.).

[17] Note that the SDF appeared as a case study in a report on "Exploring legal mechanisms for data stewardship" published by Ada Lovelace and the AI Council (2021).

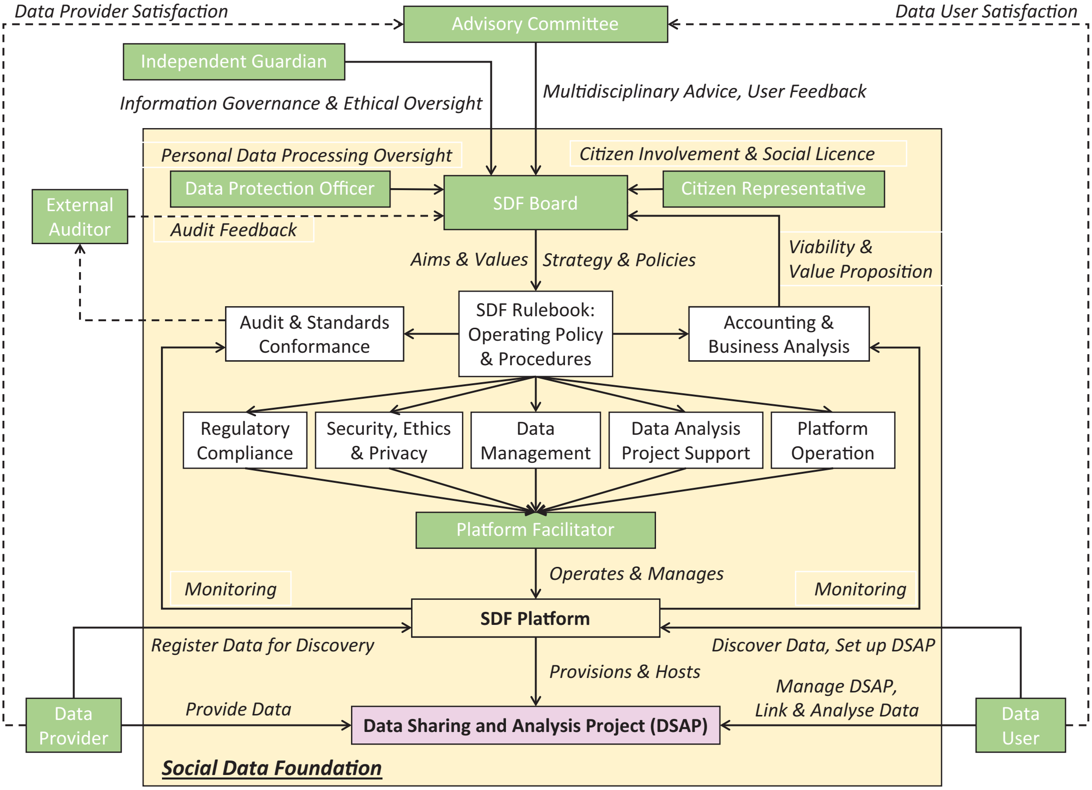
Data Provider Satisfaction
Advisory Committee
Data User Satisfaction
Independent Guardian
Information Governance & Ethical Oversight
Multidisciplinary Advice, User Feedback
Personal Data Processing Oversight
Citizen Involvement & Social Licence
Data Protection Officer
SDF Board
Citizen Representative
External Auditor
Audit Feedback
Viability & Value Proposition
Aims & Values
Strategy & Policies
SDF Rulebook: Operating Policy & Procedures
Audit & Standards Conformance
Accounting & Business Analysis
Regulatory Compliance
Security, Ethics & Privacy
Data Management
Data Analysis Project Support
Platform Operation
Platform Facilitator
Operates & Manages
Monitoring
Monitoring
SDF Platform
Register Data for Discovery
Discover Data, Set up DSAP
Provisions & Hosts
Manage DSAP, Link & Analyse Data
Provide Data
Data Provider
Data Sharing and Analysis Project (DSAP)
Data User
Social Data Foundation

Figure 1. *Social Data Foundation Governance Structure.*

- *Citizen*—an interested member of the public wanting to understand dataset use and measurable outcomes;
- *Project Manager*—a person responsible for DSAPs and ensuring legal compliance, policy compliance, and "safe people"; and
- *Data Analyst*—a person working on a DSAP analyzing datasets.

- *Data Protection Officer (DPO)*: A standard role (whose appointment in some instances is mandatory under the General Data Protection Regulation (GDPR, 2016) for organizations that process personal data to oversee the processing to ensure that it is compliant with GDPR obligations and respects data subjects' rights. For the SDF, the DPO is responsible for overseeing the processing of any personal data within the SDF and advising on compliance with the GDPR, in particular the identification and implementation of controls to address the risk of reidentification when different Data Providers' data are linked in response to Data Users' queries, thus contributing to "safe data." The DPO's advice extends to the special case of "safe return" where in some cases the outputs of projects are permitted to be returned to the Data Provider for reintegration with their source data. Here, the DPO can work with project staff and the Data Providers themselves to determine the potential for reidentification when project results are reintegrated with source data, whether reidentification is permissible, or how it can be prevented. The DPO works closely with the Independent Guardian who is responsible for overseeing the processing of all types of data.
- *External Auditor*: A body independent to the SDF who is responsible for auditing or certifying its performance, conformance to standards and/or compliance to regulations.
- *Independent Guardian*: A team of experts in data governance, who are independent from the SDF Board and oversee the administration of the SDF to ensure that all data-related activities within the SDF realize the highest standards of excellence for data governance in accordance with applicable

https://doi.org/10.1017/dap.2022.1 Published online by Cambridge University Press

policies and processes that govern the operation of the SDF Platform. In particular, the Independent Guardian shall: (a) help set up a risk management framework for data sharing; (b) assess the proposed data use cases in accordance with this risk management framework; and (c) audit and monitor all day-to-day data-related activities, including data access, citizen participation and engagement. These responsibilities contribute to "safe projects," trustworthy governance, and support SDF transparency and best practice.

- *Platform Facilitator*: An executing officer, usually supported by a team, who oversees the technical day-to-day operation of the SDF Platform, including the provision of infrastructure and functional services for Data Providers and Data Users, the implementation of governance policies, and support services for other roles where required.
- *The SDF Board*: The inclusive decision-making body whose appointed members represent the interests of the SDF's key stakeholders: Data Providers, Data Users, and Citizens. Feedback from Data Providers and Data Users is obtained via the Advisory Board, and citizen engagement is provided by the presence of Citizen Representatives as board members. The principal responsibility of its members is to administer the SDF's assets and carry out its purpose, including the determination of objectives, scope and guiding principles as well as progressive operating policies, processes and regulations through maintenance of the SDF Rulebook. The SDF Board therefore consumes multidisciplinary input from other roles and bodies—and consolidates this knowledge into the policies and processes expressed in the SDF Rulebook.

3.1.2. Examples of SDF governance processes for DSAPs

The SDF provides a "safe setting" for "safe projects"—that is, DSAPs. The following table of standard governance processes is by no means exhaustive, but provides an illustration of the types of processes that must be in place for all DSAPs (Table 1).

Table 1. *Examples of key standardized processes for all data sharing and analysis projects (DSAPs)*

	Key standardized process for all "DSAPs"	Relation to the "five safes plus one"
(a)	The SDF DSAP approval process	
	DSAPs must successfully complete a SDF pre-approval process before access is granted to the SDF Platform. A DSAP must have a Project Manager who is responsible for overseeing and administering the project, and is pre-approved by the SDF via background checks. The Project Manager must apply to the SDF and provide evidence that their project has satisfied relevant legal and ethical requirements. This evidence will be checked by the SDF governance body in accordance with the SDF Rulebook, and only if satisfactory will the SDF support the project and grant access to any specified datasets	"Safe people"; "Safe projects"
(b)	The SDF DSAP container process	
	DSAPs must be secure and isolated from other projects and data	"Safe setting"
(c)	The SDF DSAP default access policy	
	There must be a default access policy that prevents unauthorized data export or download from the secure environment	"Safe outputs"
(d)	The SDF DSAP audit trail process	
	DSAPs must have their activities recorded for audit purposes in a nonrepudiable way; a project audit record is shared between the Project Manager, the relevant Data Provider(s), and the SDF Platform	"Safe setting"

(Continued)

https://doi.org/10.1017/dap.2022.1 Published online by Cambridge University Press

Table 1. *Continued*

	Key standardized process for all "DSAPs"	Relation to the "five safes plus one"
(e)	The SDF DSAP functional anonymization process DSAPs must process data legally, ethically, and securely—in accordance with all applicable data-sharing licenses and/or agreements, ethics approvals, and all other necessary requirements. The SDF must practise "functional anonymization," which is defined by Elliot et al. (2018) as "the practice of reducing the risk of re-identification through controls on the data and its environment so that it is at an acceptably low level"	"Safe data"; "Safe projects"; "Safe setting"

3.2. Datatrust services

Datatrust services are a sociotechnical evolution that advances databases and data management systems toward a network of trusted stakeholders—who are connected through linked data by closely integrating mechanisms of governance with data management and access services. *Datatrust services* can offer a multisided service platform (the SDF Platform), which creates value through linked data interactions between Data Providers and Data Users, while implementing the necessary management and governance arrangements. We now describe the specific functionalities of our *datatrust service platform* recognizing that the features and design choices represent a specific implementation. We expect multiple implementations of *datatrust services* to emerge, each with particular characteristics, but designed to flexibly support a range of governance models and values.

3.2.1. Overview: Datatrust service platform

For illustration, Figure 2 depicts a *datatrust service platform* embedded into the "SDF Governance Model" (Section 3.1).

Some key features of this *datatrust service platform* (as depicted by Figure 2) are as follows:

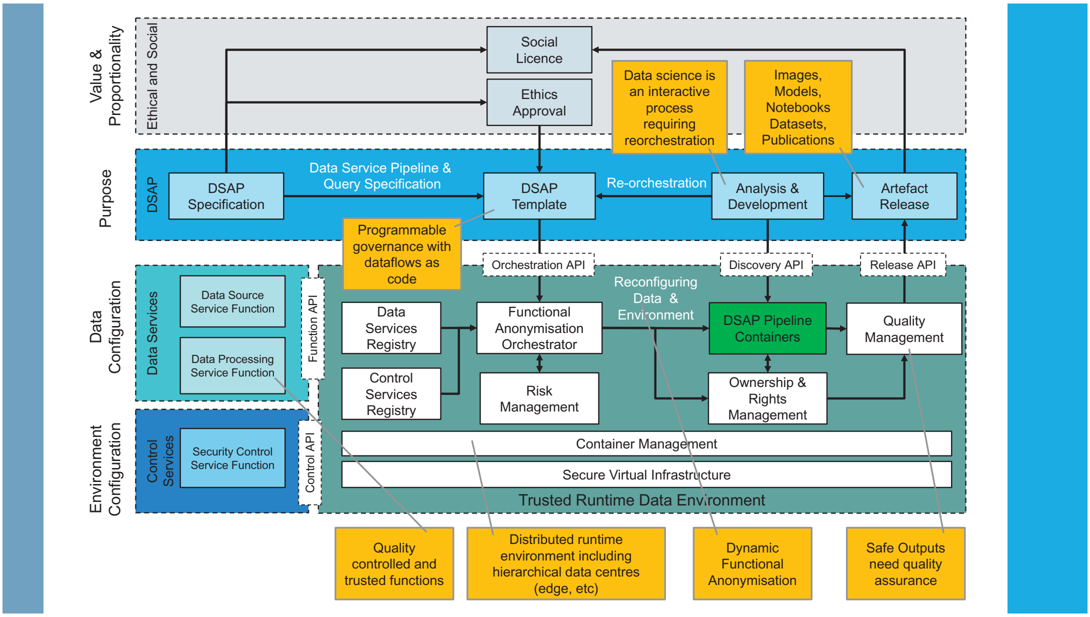
Value & Proportionality
Ethical and Social
Social Licence
Ethics Approval
Data science is an interactive process requiring reorchestration
Images, Models, Notebooks Datasets, Publications
Purpose
DSAP
DSAP Specification
Data Service Pipeline & Query Specification
DSAP Template
Re-orchestration
Analysis & Development
Artefact Release
Programmable governance with dataflows as code
Orchestration API
Discovery API
Release API
Data Configuration
Data Services
Data Source Service Function
Data Processing Service Function
Function API
Reconfiguring Data & Environment
Data Services Registry
Functional Anonymisation Orchestrator
DSAP Pipeline Containers
Quality Management
Control Services Registry
Risk Management
Ownership & Rights Management
Environment Configuration
Control Services
Security Control Service Function
Control API
Container Management
Secure Virtual Infrastructure
Trusted Runtime Data Environment
Quality controlled and trusted functions
Distributed runtime environment including hierarchical data centres (edge, etc)
Dynamic Functional Anonymisation
Safe Outputs need quality assurance

Figure 2. *A* datatrust *service platform.*

https://doi.org/10.1017/dap.2022.1 Published online by Cambridge University Press

A. *Datatrust services* related to “ensuring value and proportionality”: Such *datatrust services* are necessitated to provide oversight for the lifecycle of DSAPs—through stages of request, orchestration, knowledge discovery, and artifact release—in order to ensure “value and proportionality” within the defined remit of the SDF for stakeholder approval (i.e., maintaining a social license) and ethical oversight.

B. *Datatrust services* related to “purpose specification”: Such *datatrust services* are required to make sure the purpose of DSAPs are specified in templates that combine both human and machine-readable elements for consistency—and allow for human approval and automated deployment. Templates support programmable governance where dataflows are defined as code, and are used to orchestrate quality-controlled data services within functional anonymization environments dynamically with repeatability.

C. *Datatrust services* related to “configuration of data and environment”: Such *datatrust services* for “data configuration” and “environment configuration” are essential to give rise to the important property of functional anonymization, which is concerned with addressing risk of reidentification by controlling data and their environment:

> A data environment usually consists of four key elements, and a description of a data environment that includes these four elements is usually adequate for discussing, planning or evaluating the functional anonymisation of the original dataset. These elements are: other data [/] data users [/] governance processes [/] infrastructure (Elliot et al., 2018).

Interpreting these four key elements of the “data environment” for a DSAP:

a. “*Other data*” are further datasets within the DSAP that may be combined with the dataset in question. Each DSAP is assessed for risk of reidentification on a case-by-case basis where the specific combination of datasets and rights asserted in smart contracts are considered.
b. “*Data users*” are vetted Data Analysts (“safe people”).
c. “*Governance processes*” comprise the SDF governance processes—for example, for ethical approval, stakeholder acceptance, policy enforcement through contracts, licenses, and data usage policies associated with data service functions.
d. “*Infrastructure*” is provided by secure cloud resources to *datatrust services* that may be federated through software-defined wide area networks (SD-WANs) allowing flexible configuration of networking elements—including potential for distributed runtime environment and hierarchical data centers (e.g., public cloud, private cloud, and edge). *Datatrust services* are deployed as a cloud tenant, and utilize standard cloud services APIs in order to package containers and provision secure pipelines of containers and resources dedicated to each DSAP, which are isolated from other DSAP instances.

To enable a “safe setting” and support for “safe projects,” *datatrust services* comply with applicable cyber security certification (e.g., UK Cyber Essentials Plus) and industry-specific certification security standards (e.g., NHS Data Security and Protection Toolkit, 2021 to enable NHS health data processing). In addition, *datatrust services* are operated within a cybersecurity risk assessment and mitigation process to guard against cyber threats and attacks—guided by ISO 27005 (ISO, 2018), and compliant with ISO 27001 (ISO, 2013) risk management.

Once a DSAP is deployed, Data Users can access data services that operate on the datasets within the DSAP to produce artifacts including publications, new datasets, models, notebooks, and images. All outputs undergo quality assurance before release to academic, policy, or operational channels, including measurable evidence for social license, and updated data services available for deployment in new DSAPs.

https://doi.org/10.1017/dap.2022.1 Published online by Cambridge University Press

3.2.2. Datatrust service functionality

Datatrust services govern a wide range of data service functions to collect, curate, discover, access and process health, and social care data. The development and packaging of data service functions is conducted outside of the *datatrust service platform* by developers and then packaged as images for deployment by the platform. Such data service functions are typically quality controlled software libraries deployed by the platform depending on the requirements of Data Providers and Data Users. In general, Data Providers are required to select cohorts and prepare data at source for sharing and linking through tasks not limited to: (a) data deidentification; (b) data cleaning; (c) data quality assurance; (d) data consistency assurance (e.g., ensuring pseudonymized identifiers are consistent across datasets); and (e) data harmonization and compatibility assurance (e.g., normalizing data fields across heterogeneous data sets generated by different software). The use of standardized metadata, including provenance records, is important to make it possible to interpret and link datasets. “Health Level 7 Fast Healthcare Interoperability Resources”—known as HL7 FHIR—(Bender and Sartipi, 2013) is the predominant standard for discovery and exchange of electronic health care records and research databases, although routine datasets and those related to wider social determinants of health are vastly heterogeneous, with harmonization remaining a topic of significant research.

Data Users may (re)use a single source, or multiple sources, of data. The connection of multiple data sources is referred to as “data linking”—which is defined by the Public Health Research Data Forum (2015) as:

> bringing together two or more sources of information which relate to the same individual, event, institution or place. By combining information, it may be possible to identify relationships between factors which are not evident from the single sources.

Different data linking processes exist to combine datasets. For example, deterministic and probabilistic techniques can be used to identify the same individuals in two datasets, and then processed using cryptographic algorithms to provide tokenized link identifiers (Jones et al., 2014), while federated learning pipelines offer the opportunity to build AI (Machine Learning) models that can learn from multiple datasets without exchanging the data itself (Rieke et al., 2020).

The capability to flexibly specify, provision and monitor secure dataflow pipelines within the context of ethical oversight, social license, and risk management are key characteristics of *datatrust services.* In the following subsections, we describe four important aspects of *datatrust service* functionality in more detail: functional anonymization, specification of data and dataflows, compliance decision support, and ownership and rights management.

3.2.3. Functional anonymization

What is the “Functional Anonymization Orchestrator”? As its name suggests, the “Functional Anonymization Orchestrator” is the *datatrust service* for functional anonymization—and performs an automated process for deployment of data services, security controls/permissions, and allocation of compute storage and network resources.

How does it work? The Functional Anonymization Orchestrator interfaces with a registry of pre-approved, trusted data service functions and environment controls, as well as the Risk Management component responsible for assessment of risks related to compliance, privacy, and cybersecurity. The outcome of orchestration is an isolated and secure virtual environment for each DSAP, thus implementing “safe projects.” This combination of data configuration, environment configuration, and risk management ensures that *datatrust services* offer the property of functional anonymization—and therefore works to address its key elements, as cited by Elliot et al. (2018) (see Section 3.2.1 for further information).

https://doi.org/10.1017/dap.2022.1 Published online by Cambridge University Press

3.2.4. Specification of data and dataflows

What is the "DSAP template"? The "DSAP Template" is the *datatrust service* for the specification of data and dataflows that are subsequently used as part of ethical approvals, data-sharing agreements, and data protection impact assessments.

Table 2. *Data sharing and analysis project template types*

DSAP baseline template	Description
Platform hosted	Data are uploaded to the Platform from a Data Provider and then subsequently imported and linked within a DSAP *Applies to situations where data are hosted by the Platform only*
Project hosted	Data are uploaded and linked within a DSAP from one or more Data Providers *Applies to situations where data are made discoverable via the Platform, but are not hosted by the Platform*
Federated query	Data are hosted by a Data Provider and access is limited to analysis by predefined distributed queries executed at Data Providers and subsequent linking of results *Applies to situations where Data Providers wish to maximize control over their datasets*
Hybrid hosted and query	Data is linked in some combination of Platform Hosted, Project Hosted and Federated Query

How does it work? The Functional Anonymization Orchestrator allows Data Users to express DSAP requirements through declarative templates using cloud-native orchestration languages (e.g., Kubernetes). Such declarative languages provide ways to construct machine-readable DSAP templates that can be tailored using properties and used to provision and configure virtual instances offering the required data services. The templates include data service configuration specifying queries that define cohort inclusion and exclusion criteria, and retention policies. The standardization of templates and APIs will be essential for interoperation between *datatrust services* governing health and social care data.

Templates are technical in nature and therefore a predefined set of baseline templates are defined for different project types, as outlined in Table 2. These templates support data distribution patterns for hosting, caching, and accessing datasets—and offer the flexibility required for variability in risk of loss of control associated with different types of datasets and Data Providers' appetite for such risks. In addition, the flexibility in data distribution models allows for replication, retention, and associated cost implications to be considered.

3.2.5. Compliance decision support

What is the "risk management" component? The "Risk Management" component is the *datatrust service* for regulatory compliance decision support for DSAP pipelines—and utilizes an asset-based risk modeling approach following ISO 27001 (ISO, 2013); initially based on cyber security.

How does it work? Risk is explicitly defined in relation to *threats* upon *assets*. Assets are tangible and nontangible items of value—while datasets are core assets of interest, other assets include software, data, machinery, services, people, and reputation. Assets may be attacked by threats, which cause *misbehavior* in the asset (i.e., unwanted, erroneous, or dangerous behavior). The *risk* to the asset is the severity of the misbehavior combined with the likelihood of the threat. *Controls* may be applied to the asset to reduce the likelihood of the threat occurring.

https://doi.org/10.1017/dap.2022.1 Published online by Cambridge University Press

A semi-automated approach for risk identification and analysis based on a security risk analysis tool—the "System Security Modeller"—has been developed in previous work; and, applied to trust in communication network situations (Surridge et al., 2018) as well as health care applications and data protection compliance (Surridge et al., 2019). This work has been further extended into the realm of regulatory compliance requirements in Taylor et al. (2020). Threat types supported by the Risk Management approach therefore include cyber security, such as those associated with the "Open Web Application Security Project" (OWASP) Top Ten (2021), or compliance threats due to failures in regulatory or licensing compliance.

The Risk Management component therefore detects cyber security or regulatory compliance threats—based on a specified DSAP template—and provide recommendations for controls (mitigating strategies) to block a compliance threat sufficiently to satisfy a regulatory requirement. While further work is required on the specifics of the compliance requirements themselves, the methodology for encoding compliance requirements into a risk management approach has been proven.

Example of potential risk: Reidentification. A key risk to be mitigated is the potential for reidentification that can arise through data sharing, usage and reusage in DSAPs. Oswald (2013) defines the risk of reidentification as:

> the likelihood of someone being able to re-identify an individual, and the harm or impact if that re-identification occurred.

Data linking, "singling out" individuals, and "inference"—that is, deducing some information about an individual (Article 29 Data Protection Working Party, 2014) are data vulnerabilities that may result in potential harms to data subjects, as well as compliance threats and potential harms to Data Providers. The Risk Management component ensures that the SDF can "mitigate the risk of identification until it is remote" (Information Commissioner's Office, 2012) using control strategies (e.g., source pseudonymization and *k*-anonymization) that are assessed according to the DSAP template risk model, and monitored through risk assessment points on DSAP deployment and data service functions (e.g., upload, query, and aggregation). The Risk Management component provides risk assessment to the Functional Anonymization Orchestrator—and only if an acceptable, low level of risk is found will the services provide data to Data Users. Where an unacceptable level of risk is found, data access is denied pending further checking and additional measures to deidentify data.

Example of risk assessment points: Federated query scenario. As an example, Figure 3 shows the risk assessment points for the "Federated Query DSAP Template" (as denoted by four numbered green diamonds):

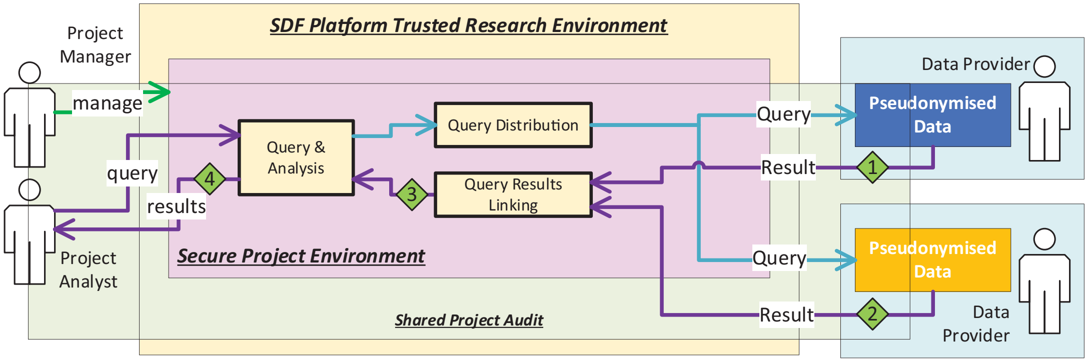

Figure 3. *Reidentification risk assessment for distributed query.*

In the Federated Query scenario (one of four predefined baseline DSAP templates outlined in Table 2), policy enforcement is dynamic with risk assessment points (1) and (2) placed at each Data Provider upon receipt and processing of a query fragment; here the results of the query fragment are checked. Risk assessment point (3) occurs after the result fragments are linked, and risk assessment point (4) occurs after any analysis of the linked result.

Note that a key difference between the Platform Hosted and Federated Query scenarios (see Table 2) is where reidentification risk assessment takes place. While, in the Federated Query scenario, some of the reidentification risk checking is distributed to Data Providers; in the Platform Hosted scenario, all such checking is undertaken by the operator of the Platform. The ability to check for reidentification risk on a per-query basis at Data Provider premises (in the Federated Query scenario) therefore strengthens the Data Provider's control over their data for circumstances where data cannot be exchanged.

3.2.6. Ownership and rights management

What is the "ownership and rights management" service? SDF Governance requires that each DSAP have its activities recorded for audit purposes in a nonrepudiable way. This *datatrust service* therefore ensures that all permitted stakeholders for a specified DSAP—for example, Project Manager, Data Provider(s)—have access to a "Shared Project Audit Distributed Ledger" where all transactions for a DSAP are recorded.

How does it work?

Distributed ledger technology. To provide such Shared Project Audit Distributed Ledgers, the SDF employs distributed ledger technology (based on blockchain technology):

> A distributed ledger is essentially an asset database that can be shared across a network of multiple sites, geographies or institutions (UK Government Chief Scientific Adviser, 2016).

Distributed ledger technology has appropriate properties for "DSAP audit" in that it is immutable (i.e., records cannot be altered or deleted), and it is inherently shared and distributed (i.e., each permitted stakeholder has their own copy of the audit record). All transactions within the DSAP (e.g., analysis activities of data analysts) are automatically recorded onto the audit ledger. Audit logs are irreversible and incontrovertible, thus providing a robust audit trail, as well as encouraging compliant behavior.

Smart contracts. To ensure compliance with all specified data-sharing agreements and/or licenses applicable to a DSAP, the Ownership and Rights Management service also employs smart contracts technology. Smart contracts are related to distributed ledger technology—as programs are run on a blockchain, which

> define rules, like a regular contract, and automatically enforce them via the code (Ethereum, 2021).

Smart contracts have several useful properties for the purposes of "license terms enforcement" in the SDF Platform:

- *Smart contracts are programs that provide user functionality*: Data browsing, analysis, access, linking, and query functions can be written within smart contracts, and used by Data Analysts in DSAPs.

  For example, a smart contract can implement data linking using pseudonymized identifiers, or queries on datasets at Data Providers.
- *Smart contracts provide means to automate enforcement of agreement terms*: Each invocation of functionality provided by smart contract programs can be evaluated at runtime—based on the combined data input, function, and parameters of the invocation—for compliance with the license terms of the Data Providers whose datasets are used in a DSAP. Smart contracts implementing data-oriented functions should be the entry point for all data analysis activity, and license terms therefore can

https://doi.org/10.1017/dap.2022.1 Published online by Cambridge University Press

be enforced at the point of execution by the Data Analyst. This automated enforcement prevents Data Analysts from executing operations that are inconsistent with the license terms of Data Providers. For example, if one Data Provider prohibits pseudonymized linking, their dataset will not be available to a smart contract implementing pseudonymized linking; whereas for other Data Providers who do permit linking, their datasets can be available to the "linking" smart contract.

- *The transactions executed for smart contracts are recorded automatically on "Shared Project Audit Distributed Ledgers"*: Given smart contracts are implemented on blockchain (i.e., the underlying technology shared with distributed ledger technology), a key link between the functionality available to data-centric functions executed by Data Analysts and the Shared Project Audit Distributed Ledger is provided.

It is important to highlight that further work is required to establish specific smart contract dataset functions and license terms to be enforced. While it is expected that there will be highly specific requirements for individual DSAPs, it also remains likely that there will be some common functionality and license terms frequently used across many types of DSAPs.

4. Validation of the SDF Model

To validate the SDF model, we now analyze a real-world project exploring the social determinants of health: the "Multidisciplinary Ecosystem to study Lifecourse Determinants of Complex Mid-life Multimorbidity using Artificial Intelligence"—MELD project (MELD, 2021). This test case seeks to answer the question: *if the MELD project were to be supported by the SDF (as a DSAP), to what extent would the features of the SDF model improve the safety, execution and impact of the project?*

4.1. Test case overview: National Institute for Health Research — MELD project

MELD focuses on the "lifecourse causes of early onset complex" multimorbidity; "early onset" is where a person has two or more long-term conditions before the age of 50 years old, and "complex" where a person has four or more long-term conditions (MELD, 2021). Multimorbidity is one of several key focus areas for health and social care transformation. A substantial number of people (30% all ages, 54% > 65 years of age and 83% > 85 years) suffer from two or more long-term conditions (Cassell et al., 2018), with those from more disadvantaged backgrounds more likely to develop multimorbidity earlier. Multimorbidity affects quality of life, leads to poorer health outcomes and experiences of care, and accounts for disproportionate healthcare workload and costs. Solutions are needed to understand disease trajectories over the life-course (start well, live well, age well) at population levels, and to develop effective personalized interventions. Furthermore, complex and heterogeneous longitudinal and routine linked data—including social determinants of health from datasets beyond electronic healthcare systems—are needed to study the clusters and trajectory of disease.

MELD is selected for validation of the SDF model as it is closely aligned with the purpose of the SDF. Specifically, MELD is seeking to develop novel public health interventions by analyzing the social determinants of health using complex linked social and health datasets. MELD is part of a multidisciplinary ecosystem for data linkage and analysis together with citizen participation and engagement. As such, MELD helps unpack different data requirements required for DSAPs—and can drive the development of DSAP templates. MELD also highlights that data linkage can take many forms, such as transfer learning, and demonstrates the variety of generated outputs that would need to be managed—for example, derived data, artificial intelligence/machine learning models, and tooling.

4.2. MELD 1.0: Initial project

The first phase of MELD brings together a multidisciplinary team—including researchers from medicine, social science, and computer science—and patient and public involvement (PPI) representatives to explore life-course determinants of multiple long-term conditions. MELD is supported by a National Institute for Health Research (NIHR) and considers two datasets:

- *The 1970 British Cohort Study (BCS70) dataset*: The BCS70 is a well-established, longitudinal birth cohort dataset that "follows the lives of more than 17,000 people born in England, Scotland and Wales in a single week of 1970." (UK Data Service, 1970) This dataset is available for secondary use via the UK Data Service. The MELD project has access to all BCS70 data collected as part of data sweeps.
- *The Care and Health Information Exchange Analytics (CHIA) dataset*: The CHIA (Care and Health Information Exchange, n.d.) is a clinical dataset provided by the NHS and includes 700,000 patients in Hampshire and the Isle of Wight. The dataset is available for secondary use via the South, Central, and West Commissioning Support Unit on behalf of health and social care organizations in Hampshire, Farnham, and the Isle of Wight.

The two datasets provided must only be accessible to the research team for the purposes of the project. The development phase has received institutional-level (the appropriate Research Ethics Committee [REC]), and national-level ethics approval (NHS REC). As part of the ethics review process, the project team has carried out a data protection impact assessment.

MELD will develop AI pipelines to:

(1) Curate the datasets to assess and ensure readiness;
(2) Develop clustering algorithms to identify early onset complex and burdensome multiple long term conditions;
(3) Explore if sentinel conditions and long-term condition accrual sequence can be identified and characterized; and
(4) Devise AI transfer learning methods that allow extrapolation of inferences from BCS70 to CHIA —and vice versa.

The intention is for MELD to link together more datasets, in particular those related to other birth cohorts and larger routine datasets requiring "the necessary environment, principles, systems, methods and team in which to use AI techniques" in order to "identify optimal timepoints for public health interventions" (IT Innovation Centre, n.d.).

The exploratory work undertaken will be used as a proof of concept for a larger research collaboration application:

> to scale the MELD ecosystem to 'combine' other birth cohorts and larger routine datasets giving much greater power to fully explore the lifecourse relationship between sequence of exposure to wider determinants, sentinel and subsequent clinical events, and development of early other complex MLTC-M clusters (MELD, 2020).

It is therefore vital that MELD is able to handle more complex types of data linkage activities than the remit of its current study—for example, combinations of multiple types of diverse data from additional data providers with different licensing arrangements, provenance, and quality. As part of these future work plans, MELD requires a data governance model that is scalable and adaptive to its growing needs.

4.3. Hypothetical MELD 2.0: Scaling up data linking facilitated by the SDF

The SDF *datatrust services* will support the MELD project team in the delivery of research outcomes while helping stakeholders manage associated risks efficiently. The stakeholders include: the NHS Health Research Authority (HRA); the two data providers (NHS for CHIA and the UK Data Service for BCS70); the principal investigator for MELD—who takes the role of project manager; and the data analysts working on the project.

https://doi.org/10.1017/dap.2022.1 Published online by Cambridge University Press

4.3.1. Project approvals, data access and resources

The principal investigator for MELD must first establish the required research ethics approvals (e.g., at institutional and national levels), data access rights, and resources to undertake research—all of which are necessary to delegate rights to Data Analysts as part of the MELD project team. For instance, NHS HRA approval "applies to all project-based research taking place in the NHS in England and Wales" (NHS HRA, 2021). NHS HRA approval requires researchers to submit a research application form through the IRAS—which includes detailed study information along with supporting documents (NHS HRA, 2019, 2021)—such as, "Organization Information Document," "Schedule of Events" and "Sponsors Insurance" provided by the principal investigator's host organization following local approval.

While institutional and national governance processes for approval requests require similar information, there is little standardization between processes and document structures. Consistency between described dataflows, data scope, policies, and environments is entirely disconnected from system implementation. By starting with a project template configured with human and machine-readable data requirements, dataflows, and environment controls (e.g., the DSAP template as described in Section 3.2.4), risk management can be directly embedded into research processes—and thus greater agility in such processes can be achieved. The project specification is then used and adapted to authority requests. Ideally, authorities need to transform governance web forms to programmable APIs and business processes; collaboration through standardization will be required.

4.3.2. Example: Setup and operation of a MELD 2.0 DSAP

We now outline the main steps to be taken by the principal investigator for MELD and the SDF in order to set up a DSAP for MELD 2.0.

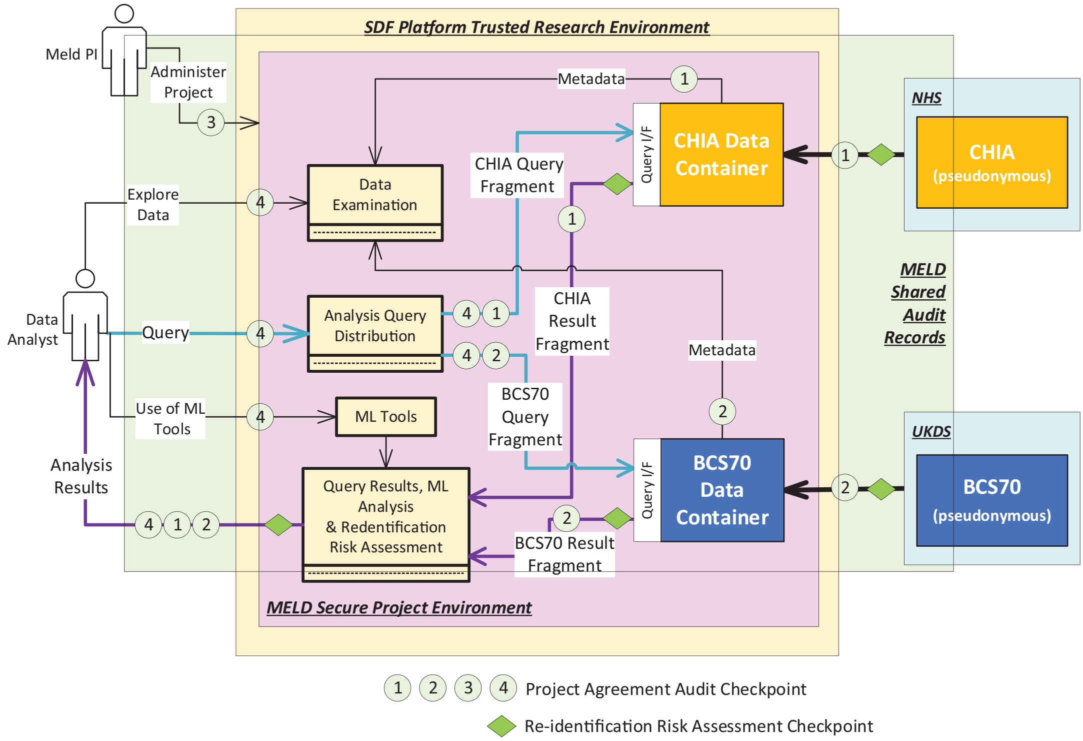

Figure 4. *MELD within the* datatrust *service platform.*

Figure 4 shows the secure project environment for the MELD 2.0 project within the SDF platform. During *setup*, the following steps occur:

(1) The principal investigator for MELD ("MELD PI") requests a DSAP—and then completes a DSAP template with data configuration (inclusion, exclusion, and retention) along with supporting information regarding satisfaction of compliance requirements, ethical soundness and social benefit.
(2) The SDF's governing body performs background checks on the principal investigator for MELD —and if approved assesses the project application.
(3) The SDF's governing body assesses the application and if the evidence regarding compliance, ethics, and social benefit is satisfactory, the SDF agrees to support MELD.
(4) The principal investigator for MELD makes an agreement with the SDF for a DSAP (as denoted by the "green circle 3" in Figure 4).
(5) The SDF creates a DSAP for MELD. The MELD DSAP (represented by the "pink box" in Figure 4) is a secure environment—isolated from DSAPs for other projects. Access to the MELD DSAP for data analysts is specified by principal investigator for MELD and enforced by the platform.
(6) The principal investigator for MELD acquires agreements and/or licenses from specified data providers, which will come with terms of use that must be respected (indicated by the "green circles 1 and 2," respectively in Figure 4). The MELD principal investigator names the SDF as their TRE in agreement with these specified data providers.
(7) The datasets are acquired from the Data Providers by the SDF (as the named delegate by the principal investigator)—and are loaded into the MELD DSAP.
(8) The principal investigator for MELD authors the "MELD Data Usage Policy" (as denoted by "green circle 4" in Figure 4), which must be consistent with the licenses and/or agreements between the principal investigator for MELD and the two data providers ("green circles 1 and 2" in Figure 4).
(9) The principal investigator for MELD appoints Data Analysts, who must agree to the "MELD Data Usage Policy."
(10) The principal investigator for MELD grants access to the "MELD DSAP" for each approved Data Analyst.

During *operation*, the following steps are performed, most likely iteratively. All MELD analyst operations are via *datatrust services* that perform data functions encoded within smart contracts that provide functionality constrained to agreements and policies for MELD, which are denoted by the "green circles" in Figure 4.

(1) One or more specified Data Analysts for MELD explore dataset metadata limited by those defined in the DSAP specification.
(2) One or more specified Data Analysts for MELD formulate queries, which may be on an individual dataset or inferences between datasets. These queries must be consistent with:

  a. Specified data usage terms for the DSAP; and
  b. Approvals (IRAS for CHIA dataset; UK Data Service End User Agreement for BCS70 dataset).

(3) One or more specified Data Analysts for MELD run queries and use machine learning tools to analyze the resultant data. Depending on the query from the Data Analyst(s), the results may be from one dataset or both datasets linked by common attributes. Data Analysts are not able to download the datasets from the DSAP.
(4) Results are returned after internal checking for consistency with the appropriate agreements. Audit records (the "large shared green box" in Figure 4) are maintained and shared between the key stakeholders to encourage transparency and promote trustworthiness.

https://doi.org/10.1017/dap.2022.1 Published online by Cambridge University Press

4.4. Validation

The SDF model aims to improve and accelerate data flows for health and social care transformation in five ways (Boniface et al., 2020), through: "empowerment of citizens"; "greater assurances to stakeholders"; "faster ethical oversight and information governance"; "better discoverability of data and generated outcomes"; and "facilitation of localized solutions with national leadership." We now explore each proposed benefit—and how it can be realized for the MELD project.

4.4.1. Empowerment of citizens

Given the depth of data required to understand lifestyle behaviors, socioeconomic factors, and health, the development of AI-based interventions addressing multimorbidity over the life-course necessitates a trusted partnership with citizens: access to such data is contingent on trust building.

The SDF model is governed through the principles and values of open science, ethics, integrity, and fairness in full consideration of digital inclusion (i.e., literacy and innovation opportunities), social inclusion, and gender equality. It further considers the structures required to support multidisciplinary and multimotivational teams. Through Citizen Representatives, patient/service user voice is represented at board level. Citizen empowerment is further addressed through collaborations with local initiatives, such as the Southampton Social Impact Lab (2021), which allows for novel ways of codesign and coevaluation, including hard-to-reach groups. The SDF model therefore goes beyond representation in governance—and further facilitates participation in the design of solutions for communities.

The SDF is positioned in Southampton (UK)—a region serving a 1.8 million population (3.7 million including specialist care) with a large network of distributed health and social care providers. The geographic region and environmental conditions are highly diverse—including urban, maritime, and rural economic activities as well as large permanent/transient populations presenting a diverse population with a wide range of health and care needs. This population diversity helps to ensure civil and citizen engagement activities (e.g., patient/service user voice, codesign, and coevaluation), related to the discovery and evaluation of new interventions, as inclusive and connected to local needs. The SDF is therefore well positioned to make sure that research results are publicized appropriately, and that community and individual benefits are realized—with evidence provided of proven potential.

4.4.2. Greater assurances for stakeholders

The design, testing, and generalization of interventions from MELD require the incremental exploration of the datasets required to develop new clustering and prediction algorithms. The methodology requires an iterative process of data discovery, curation, and linking to assess the readiness of datasets for the required analysis. The quality of routine health and social care data, and birth cohort data is unknown, as is the performance of AI pipelines applied to such data. As such, data needs to be carefully assembled, incrementally, in accordance with governance requirements for data minimization and mitigation of risk.

The approach of the SDF to *dynamic functional anonymization, risk management, and auditable processes* is ideally designed to efficiently support projects such as MELD and provide assurances for stakeholders. Both the CHIA and BCS70 datasets are pseudonymized, and therefore present a risk of reidentification when analyzed or linked, with newly identified datasets introducing further risks. The SDF provides checkpoints for such risks within data pipelines from source to insight, and data analysis functionality constrained to compliance with license terms of Data Providers. Further, given that the SDF supports Federated Query project types, data are not linked until the purpose is known (i.e., to meet the principle of purpose limitation), the prior knowledge of the project purposes, usage context and dataset structures involved can inform the reidentification risk assessment. The use of transparent, shared, nonrepudiable audit records encourages compliant behaviors. Audit checkpoints for recording access to datasets can be verified against their respective license agreements. In some cases, multiple agreements

https://doi.org/10.1017/dap.2022.1 Published online by Cambridge University Press

are audited at the same point—for example, when the Data Analyst receives query results, the two license agreements plus data usage policy terms are audited. With all datasets stored within an isolated and secure project environment, Data Analysts are not able to download them. The datasets therefore cannot be propagated further, thus reducing the risk of unauthorized access, and potential loss of control experienced by Data Providers.

4.4.3. Faster ethical oversight and information governance

The initial MELD project is a form of "data release" where datasets (CHIA and BSC70) are defined in advance at the start of the project—and a single ethics approval is provided. In many ways, the datasets and governance of the MELD 1.0 project are simple—however, this initial approach does not scale when the complexity of data linkage increases (i.e., MELD 2.0) raising challenges for capturing the data requirements, but also providing the information to those responsible for ethical oversight, such as the NHS HRA and research sponsors.

The SDF model addresses the sociotechnical interface between humans responsible for ethics decisions and the machines used by analysts to undertake the research. By establishing the concept of DSAP templates—as a sociotechnical integration mechanism driving oversight, risk management, and provisioning—processes can be semi-automated in ways that ensure the human-in-the-loop is retained. The automation of processes will deliver efficiencies in approvals, risk assessment (e.g., deidentification standards) and dataflows, and such efficiencies will allow for the potential for iterative ways of working and reorchestration of DSAP projects when new requirements are discovered. Given the SDF model is predicated on strong oversight and monitoring of approved projects through the Independent Guardian, the SDF is able to help to support and present the exploratory work undertaken during a proof of concept. This is because the SDF is able to provide assurances to data providers that licensing arrangements were complied with, and best practice was followed.

4.4.4. Better discoverability of data and generated outcomes

MELD is part of a wider National Institute for Health Research (NIHR) AI programme, which itself is part of a vibrant research community seeking ways by which AI solutions can deliver better care. Collaboration and sharing outcomes therefore will be an essential part of MELD success and impact.

The SDF supports an ecosystem for data-driven research and innovation in health and social care. As a hub, the SDF provides opportunities for MELD to connect with a community of stakeholders sharing common interests (including local social and healthcare data providers), and experts from a wide range of disciplines, such as ethics, law, psychology, sociology, and technology. By joining the SDF community, MELD will be enriched through increased citizen engagement and participation, and feedback from the research and innovation community can uncover new associations between projects (including projects that are already part of the SDF and from elsewhere), and lead to new opportunities for collaborations and impact. More general outcomes—such as new datasets, data usage metrics, reusable methodologies, tools , and models—are all possible benefits to the community that can increase MELD impact. For example, as a progressive data governance model, the SDF would aim to iteratively learn and integrate best practices from the MELD project to influence policy, benefit the SDF community, and provide evidence for a social license.

4.4.5. Facilitation of localized solutions with national leadership

MELD aims to provide community and individual benefits to those living with multimorbidity—and must develop interventions in ways that both connect with the local needs of citizens and can be generalized and scaled nationally.

The SDF recognizes that disruptive research and innovation often happens between trusted local partners working in placed-based systems who address identified challenges together (NHS, n.d.).

https://doi.org/10.1017/dap.2022.1 Published online by Cambridge University Press

Projects are undertaken in the context of supportive national policies—where engagement in scale-up programs turns federated place-based transformation into national assets. This contrasts with approaches to build single solutions nationally, which expect place-based systems to accept and adopt them. The SDF therefore supports projects where experimentation is needed to explore unknown solutions, and retain pluralism of research, while developing leaders that have influence on the national stage.

4.5. Limitations

Although the MELD project has provided an initial validation of the SDF platform as a real-life implementation for a TRE, there are some limitations. First, since one of the MELD project coinvestigators also coleads the SDF project, it is possible that data governance constructs may have influenced each project implicitly. However, we maintain that such overlap demonstrates that the SDF is based on experience and not just a literature review. Secondly, focusing on one test case does not cover the breadth of challenges related to data linkage for health and social care transformation. For instance, the management of multiple long-term conditions is only one area of the much larger field of health and social care transformation, the data users are only from one academic institution, and there are no transnational data-sharing activities. However, notwithstanding these limitations and for the purposes of this article, we consider that as a "thought-exercise" the MELD test case provides a useful contribution to the much wider and on-going effort of the SDF initiative to test and validate the SDF model.

5. Conclusion

The SDF model provides one example of a TRE, which offers a new approach to data-driven transformation of health and social care systems that is secure, rights respecting, and endorsed by communities. Through *datatrust services*—a sociotechnical evolution of databases and data management systems—stakeholder-sensitive data governance mechanisms are combined with data services to create TREs that adhere to the "Five Safes Plus One." In an age of increasing data complexity and scale, such TREs can accelerate research and innovation that depends on multistakeholder linked data (e.g., social determinants of health research) while providing a trust-enhancing and well-regulated structure offering assurances to data subjects and data providers. The ability of *datatrust services* to dynamically orchestrate secure dataflows with properties of functional anonymization and monitor risks at runtime—allows for progressive governance models, and more iterative knowledge discovery processes. The means to iterate creates new ways to incorporate collective ethical oversight and citizen participation (i.e., representation, codesign, and evaluation) more naturally into phases of research.

We further outlined the "SDF Governance Model," including the institutional structure, processes, and roles with consideration of the full range of relevant legitimate interests and the fiduciary ethical virtues of loyalty and care. We then described how *datatrust services* can support DSAPs using capabilities of functional anonymization orchestration, risk management, and auditable data ownership and rights management. We then validated the approach against a representative project "MELD" exploring the social determinants of multimorbidity over the life-course—as an exemplar DSAP—in order to highlight how MELD can benefit from the SDF model when scaling the research to more complex datasets.

In this article, we have presented our version of *datatrust services* within the specific context of the SDF. However, we recognize that there is no-one-size-fits-all approach, and there may be simpler and more complex forms of *datatrust services* better suited to other data-sharing initiatives with different governance arrangements to the SDF (e.g., with other data-sharing purposes, contexts, diameters of trust, and stakeholder expectations). While we must remain cognizant of the types of values embedded in the design of *datatrust services*, and the extent to which these could act as constraints if redeployed in other multiparty sharing scenarios, elements of the SDF model could be used as primitives for *datatrust services* as part of other TREs. The design and development of these *datatrust services* therefore must be suitably

https://doi.org/10.1017/dap.2022.1 Published online by Cambridge University Press

flexible so that they can be generalized to deliver different governance arrangements and facilitate safe data sharing within other settings and domains.

Following agreement of the three principal partners, we now move into a phase of establishing a SDF in Southampton working with citizens to attain social license, and other stakeholders to provision infrastructure and *datatrust services.* A set of transformation projects have been identified beyond the initial MELD project that aim to deliver a wide range of benefits to citizens, healthcare providers, and social care providers, but are also being used to drive forward approaches to governance. This interplay between "progressive digitalisation" and "progressive governance" is at the heart of the SDF model, which aims to ensure that governance reflects the values and priorities of the community, in order to accelerate projects so that outcomes benefit citizens as soon as possible.

Glossary

For the purposes of this article, we define the following terms:

Data governance mechanisms	Well-defined roles and processes for ensuring the safe and secure sharing, usage and reusage of health and social care data as part of a TRE, such as in relation to collective-centric decision-making, citizen representation, and data stewardship.
Data sharing and analysis project ("DSAP")	A health and social care research project that is approved by the SDF Governance Board for facilitation via the SDF Platform.
Datatrust services	A sociotechnical evolution that advances databases and data management systems, and brings together stakeholder-sensitive data governance mechanisms with data services to create a TRE.
Fiduciary ethical virtues of loyalty and care	Behavior seen to be trustworthy, that retains trust and, in so doing, delivers positive outcomes across the full range of stakeholders in relation to a data institution (such as the SDF).
Functional anonymization	The practice of mitigating the risk of reidentification to a remote level by implementing "controls on data and its environment" (Elliot et al., 2018).
Health and social care transformation	The progressive digitalization of health and social care services in response to societal demands and advances in clinical practice, medicine, and technology.
Multimorbidity	The cooccurrence of two or more long-term health conditions.
Social Data Foundation for Health and Social Care ("the SDF")	A new data institution for multiparty data sharing to enable positive health and social care transformation via a TRE, which is based on a specific implementation of *datatrust services*.
Social determinants of health	Nonmedical factors that significantly affect individual well-being and health inequalities—for example, education and employment.
Social license	A high degree of social legitimacy; stakeholder approvals for health and social care research, innovation and transformation given to data institutions (which are under constant reevaluation)—on the basis that the main stakeholders perceive that what is being done is acceptable, trustworthy, and beneficial toward the communities it intends to serve.
Trusted research environment	A safe and secure data platform for approved DSAPs that can be accessed (remotely) by authorized persons (e.g., data analysts); and, which abides by the "Five Safes Plus One" approach: "safe people," "safe projects," "safe data," "safe setting," "safe outputs," and (where necessary) "safe return" (The UK Health Data Research Alliance, 2020).

Acknowledgments. This article expands and extends the concepts in our Web Science Institute (WSI) white paper (Boniface et al., 2020). We therefore give special thanks to all those that supported and contributed to this white paper. This includes Rachel Bailey (University Hospital Southampton NHS Foundation Trust), Tom Barnett (Web Science Institute, University of Southampton), Prof. Sally Brailsford (CORMSIS, University of Southampton), Guy Cohen and Marcus Grazette (Privitar), Paul Copping (Sightline Innovation), Christine Currie (CORMSIS, University of Southampton), Jo Dixon (Research and Innovation Services, University of Southampton), Dan King (Southampton City Council), Alison Knight (Research and Innovation Services, University of Southampton), Prof. Kieron O'Hara (Electronics and Computer Science, University of Southampton), Alistair Sackley (Web Science Institute, University of Southampton), Prof. Mike Surridge (IT Innovation Centre, University of Southampton), Neil Tape (University Hospital Southampton NHS Foundation Trust), Gary Todd (Famiio Ltd.), and Wally Trenholm (Sightline Innovation). We also greatly acknowledge the valuable discussions and feedback from Privitar on an earlier draft of the white paper, and the

https://doi.org/10.1017/dap.2022.1 Published online by Cambridge University Press

support of Pinsent Mason lawyers in the development of legal arrangements. We again thank Prof. Kieron O'Hara for the discussions and valuable input on the notion of fiduciary ethical virtues in relation to *datatrust services.* Finally, but by no means least, we extend our special thanks to NIHR MELD lead investigators, Dr. Simon Fraser and Dr. Nisreen Alwan at the University of Southampton for the contribution to the validation case. Please note that all views and opinions expressed in this article are those of the authors, and do not necessarily represent those named above. A pre-print version of this article is available via EPrints Soton—Boniface et al. (2021). Prof. Dame Wendy Hall also delivered a keynote speech, which is available via the Sixth International Data for Policy Conference playlist (Hall, 2021).

Funding Statement. The Social Data Foundation (SDF) project is partly funded and supported by the University of Southampton's Web Science Institute (WSI) and Southampton Connect. This research article has also been supported in part by the "Multidisciplinary Ecosystem to Study Lifecourse Determinants of Complex Mid-life Multimorbidity using Artificial Intelligence" (MELD) project funded by the National Institute for Health Research (Award ID: NIHR202644).

Competing Interests. The authors declare no competing interests exist.

Author Contributions. Conceptualization: M.B., L.C., B.P., S.S.-B, S.T.; Methodology: M.B., S.S.-B.; Writing—original draft: M.B., L.C., B.P., S.S.-B, S.T.; Writing—review and editing: M.B., L.C., W.H., B.P., S.S.-B., S.T. These author contributions are based on the CRedit Taxonomy—available at: https://casrai.org/credit/. All authors approved the final submitted draft.

Data Availability Statement. As part of the MELD test case, the two following datasets are discussed: the 1970 British Cohort Study (BCS70) dataset available from the UK Data Service (beta.ukdataservice.ac.uk/datacatalogue/series/series?id=200001); and, the Care and Health Information Exchange Analytics (CHIA) dataset available from the South, Central and West Commissioning Support Unit on behalf of health and social care organizations in Hampshire, Farnham, and the Isle of Wight (https://careandhealthinformationexchange.org.uk/). Restrictions apply to the availability of these data.

References

Abrams EM and Szefler SJ (2020) COVID-19 and the impact of social determinants of health. *The Lancet Respiratory Medicine 8* (7), 659–661. https://doi.org/10.1016/S2213-2600(20)30234-4

Ada Lovelace and the AI Council (2021) Exploring legal mechanisms for data stewardship. Available at https://www.adalovelaceinstitute.org/report/legal-mechanisms-data-stewardship/ (accessed 20 May 2021).

Ainsworth J and Buchan I (2015) Combining health data uses to ignite health system learning. *Methods of Information in Medicine 54*(6), 479–487. Available at https://www.thieme-connect.de/products/ejournals/pdf/10.3414/ME15-01-0064.pdf (accessed 20 May 2021).

Aitken M, Tully MP, Porteous C, Denegri S, Cunningham-Burley S, Banner N, Black C, Burgess M, Cross L, van Delden J, Ford E, Fox S, Fitzpatrick N, Gallacher K, Goddard C, Hassan L, Jamieson R, Jones KH, Kaarakainen M, Lugg-Widger F, McGrail K, McKenzie A, Moran R, Murtagh MJ, Oswald M, Paprica A, Perrin N, Richards EV, Rouse J, Webb J and Willison DJ (2020) Consensus statement on public involvement and engagement with data-intensive health research. *International Journal of Population Data Science 4*(1), 586. https://doi.org/10.23889/ijpds.v4i1.586

Arbuckle L and Ritchie F (2019) The five safes of risk-based anonymization. *IEEE Security & Privacy 17*(5), 84–89. https://doi.org/10.1109/MSEC.2019.2929282

Article 29 Data Protection Working Party (2014) Opinion 05/2014 on anonymisation techniques. WP216 adopted on 10 April 2014. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (accessed 21 May 2020).

Banner N (2020) A new approach to decisions about data. Understanding patient data. Available at https://understandingpatientdata.org.uk/news/new-approach-decisions-about-data (accessed 20 May 2021).

Bender D and Sartipi K (2013) HL7 FHIR: An Agile and RESTful approach to healthcare information exchange. In Pereira Rodrigues P, Pechenizkiy M, Gama J, Cruz Correia R, Liu J, Traina A, Lucas P and Soda P (eds), *Proceedings of the 26th IEEE International Symposium on Computer-based Medical Systems*, University of Porto, Portugal. Institute of Electrical and Electronics Engineers, Inc. (IEEE), pp. 326–331. https://doi.org/10.1109/CBMS.2013.6627810

Boniface M, Carmichael L, Hall W, Pickering B, Stalla-Bourdillon S and Taylor S (2020) A blueprint for a social data foundation: Accelerating trustworthy and collaborative data sharing for health and social care transformation. Web Science Institute (WSI) White Paper #4. Available at www.socialdatafoundation.org/ (accessed 20 May 2021).

Boniface M, Carmichael L, Hall W, Pickering B, Stalla-Bourdillon S and Taylor S (2021) The social data foundation model: Facilitating health and social care transformation through *datatrust* services. [Preprint]. Local EPrints ID: 449699. Available at http://eprints.soton.ac.uk/id/eprint/449699 (accessed 15 June 2021).

Burström B and Tao W (2020) Social determinants of health and inequalities in COVID-19. *European Journal of Public Health 30* (4), 617–618. https://doi.org/10.1093/eurpub/ckaa095

Burton PR, Murtagh MJ, Boyd A, Williams JB, Dove ES, Wallace SE, Tassé A-M, Little J, Chisholm RL, Gaye A, Hveem K, Brookes AJ, Goodwin P, Fistein J, Bobrow M and Knoppers BM (2015) Data safe havens in health research and healthcare. *Bioinformatics 31*(20), 3241–3248. https://doi.org/10.1093/bioinformatics/btv279

Care and Health Information Exchange (CHIE) (n.d.) Available at https://careandhealthinformationexchange.org.uk/ (accessed 20 May 2021).

CARE Principles for Indigenous Data Governance (2018) International data week and research data alliance plenary co-hosted event. Indigenous Data Sovereignty Principles for the Governance of Indigenous Data Workshop, Gaborone, Botswana. Available at https://www.gida-global.org/care (accessed 20 May 2021).

Carter P, Laurie GT and Dixon-Woods M (2015) The social licence for research: why *care.data* ran into trouble. *Journal of Medical Ethics 41*(5), 404–409. Available at https://jme.bmj.com/content/41/5/404 (accessed 20 May 2021).

Cassell A, Edwards D, Harshfield A, Rhodes K, Brimicombe J, Payne R and Griffin S (2018) The epidemiology of multimorbidity in primary care: A retrospective cohort study. *British Journal of General Practice 68*(669), e245–51. https://doi.org/10.3399/bjgp18X695465

Central Digital and Data Office (2020) Data ethics framework. UK Government Digital Services. Available at https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework-2020 (accessed 20 May 2021).

Centre for Data Ethics and Innovation (2020) Addressing public trust in public sector data use. Available at https://www.gov.uk/government/publications/cdei-publishes-its-first-report-on-public-sector-data-sharing/addressing-trust-in-public-sector-data-use (accessed 20 May 2021).

CurvedThinking (2019) Understanding public expectations of the use of health and care data. Developed in consultation with: Understanding Patient Data, Commissioned by One London. Available at https://understandingpatientdata.org.uk/sites/default/files/2019-07/Understanding%20public%20expectations%20of%20the%20use%20of%20health%20and%20care%20data.pdf (accessed 20 May 2021).

Data Linkage Western Australia (2021) Available at https://www.datalinkage-wa.org.au/ (accessed 19 March 2021).

Data Protection Act (2018) (UK) Available at https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (accessed 24 May 2021).

Davidson S, McLean C, Treanor S, Aitken M, Cunningham-Burley S, Laurie G, Pagliari C and Sethi N (2013) Public acceptability of data sharing between the public, private and third sectors for research purposes. Scottish Government Social Research, Ipsos MORI Scotland and University of Edinburgh, Research Commissioned by the Scottish Government. Available at https://www.webarchive.org.uk/wayback/archive/3000/ and https://www.gov.scot/resource/0043/00435458.pdf (accessed 14 December 2021).

Desai Y, Ritchie F and Welpton R (2016) Five safes: Designing data access for research. *UWE, Economics Working Paper Series 1601.* Available at https://www2.uwe.ac.uk/faculties/bbs/Documents/1601.pdf (accessed 21 May 2021).

Dodds L, Szász D Keller JR, Snaith B and Duarte S (2020) Designing sustainable data institutions. Open Data Institute (ODI) report. Contributions from Hardinges J and Tennison J. Available at https://theodi.org/article/designing-sustainable-data-institutions-paper/ (accessed 20 May 2021).

Elliot M, O'Hara K, Raab C, O'Keefe CM, Mackey E, Dibben C, Gowans H, Purdam K and McCullagh K (2018) Functional anonymisation: Personal data and the data environment. *Computer Law & Security Review 34*(2), 204–221. https://doi.org/10.1016/j.clsr.2018.02.001

Ethereum (2021) Introduction to smart contracts. Available at https://ethereum.org/en/developers/docs/smart-contracts/ (accessed 21 May 2021).

European Commission (2019) Building trust in human-centric artificial intelligence. Communication from the Commission to the European parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. COM (2019) 168 final. Available at https://digital-strategy.ec.europa.eu/en/library/communication-building-trust-human-centric-artificial-intelligence (accessed 21 May 2021).

Ford E, Boyd A, Bowles JKF, Havard A, Aldridge RW, Curcin V, Greiver M, Harron K, Katikireddi V, Rodgers SE and Sperrin M (2019) Our data, our society, our health: A vision for inclusive and transparent health data science in the United Kingdom and beyond. *Learning Health Systems 3*(3), e10191. https://doi.org/10.1002/lrh2.10191

Galea S, Abdalla SM and Sturchio JL (2020) Social determinants of health, data science, and decision-making: Forging a transdisciplinary synthesis. *PLoS Medicine 17*(6), e1003174. https://doi.org/10.1371/journal.pmed.1003174

Geissbuhler A, Safran C, Buchan I, Bellazzi R, Labkoff S, Eilenberg K, Leese A, Richardson C, Mantas J, Murray P and De Moor G (2013) Trustworthy reuse of health data: A transnational perspective. *International Journal of Medical Informatics 82* (1), 1–9. https://doi.org/10.1016/j.ijmedinf.2012.11.003

General Data Protection Regulation (GDPR) (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) European Commission. Available at https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed 21 May 2021).

Hall W (2021). A Blueprint for a Data Foundation. Keynote Speech at Sixth International Data for Policy Conference 2021. Recording available at https://dataforpolicy.org/global-discussion-on-the-future-of-policy-data-interactions-at-data-for-policys-sixth-edition/ (accessed 17 December 2021).

Harrison T (2020) Putting the trust in trusted research environments. Understanding patient data. Available at https://understandingpatientdata.org.uk/news/putting-trust-trusted-research-environments (accessed 21 May 2021).

Hawkes N (2013) Hospitals without walls. *BMJ 34*, f5479. https://doi.org/10.1136/bmj.f5479

Hripcsak G, Bloomrosen M, FlatelyBrennan P, Chute CG, Cimino J, Detmer DE, Edmunds M, Embi PJ, Goldstein MM, Hammond WE, Keenan GM, Labkoff S, Murphy S, Safran C, Speedie S, Strasberg H, Temple F and Wilcox AB (2014)

Health data use, stewardship, and governance: Ongoing gaps and challenges: A report from AMIA's 2012 Health Policy Meeting. *Journal of the American Medical Informatics Association 21*(2), 204–211. https://doi.org/10.1136/amiajnl-2013-002117

ICES (2021) Available at https://www.ices.on.ca/ (accessed 20 May 2021).

Information Commissioner's Office (ICO) (2012) Anonymisation: Managing data protection risk code of practice. Available at https://ico.org.uk/media/1061/anonymisation-code.pdf (accessed 20 May 2021).

Integrated Research Application System (IRAS) (2021) Available at https://www.myresearchproject.org.uk/ (accessed 20 May 2021).

ISO (2013) ISO/IEC 27001:2013. Information technology—Security Techniques—Information security management systems—Requirements, International Organization for Standardization, 2013. Available at https://www.iso.org/ (accessed 20 May 2021).

ISO (2018) ISO 27005 Information Technology—Security techniques—Information security risk management. Available at https://www.iso.org/ (accessed 20 May 2021).

IT Innovation Centre (n.d.) MELD. University of Southampton. Available at http://www.it-innovation.soton.ac.uk/projects/ai-meld (accessed 4 June 2021).

Jacobs B and Popma J (2019) Medical research, big data and the need for privacy by design. *Big Data & Society 6*, 1–5. https://doi.org/10.1177/2053951718824352

Janssen M, **Brous P**, **Estevez E**, **Barbosa LS and Janowski T** (2020) Data governance: Organizing data for trustworthy artificial intelligence. *Government Information Quarterly 37*(3), 101493. https://doi.org/10.1016/j.giq.2020.101493

Jones KH and Ford DV (2018) Population data science: Advancing the safe use of population data for public benefit. *Epidemiology and Health 40*, e2018061. https://doi.org/10.4178/epih.e2018061

Jones KH, **Ford DV**, **Jones C**, **Dsilva R**, **Thompson S**, **Brooks CJ**, **Heaven ML**, **Thayer DS**, **McNerney C and Lyons RA** (2014) A case study of the Secure Anonymous Information Linkage (SAIL) gateway: A privacy-protecting remote access system for health-related research and evaluation. *Journal of Biomedical Informatics 50*, 196–204. https://doi.org/10.1016/j.jbi.2014.01.003

Kariotis T, **Ball M**, **Greshake Tzovaras B**, **Dennis S**, **Sahama T**, **Johnston C**, **Almond H and Borda A** (2020). Emerging health data platforms: From individual control to collective data governance. *Data & Policy 2*, E13. https://doi.org/10.1017/dap.2020.14

Lin D, **Crabtree J**, **Dillo I**, **Downs RR**, **Edmunds R**, **Giaretta D**, **De Giusti M**, **L'Hours H**, **Hugo W**, **Jenkyns R**, **Khodiyar V**, **Martone ME**, **Mokrane M**, **Navale V**, **Petters J**, **Sierman B**, **Sokolova DV**, **Stockhause M and Westbrook J** (2020) The TRUST principles for digital repositories. *Scientific Data 7*, 144. https://doi.org/10.1038/s41597-020-0486-7

Marmot M, **Allen J**, **Boyce T**, **Goldblatt P and Morrison J** (2020) *Health Equity in England: The Marmot Review 10 Years on*. London: Institute of Health Equity. Available at http://www.instituteofhealthequity.org/resources-reports/marmot-review-10-years-on/the-marmot-review-10-years-on-full-report.pdf (accessed 21 May 2021).

Mayer RC, **Davis JH and Schoorman FD** (1995) An integrative model of organizational trust. *The Academy of Management Review 20*(3), 709–734. Available at https://www.jstor.org/stable/258792 (accessed 21 May 2021).

MedConfidential (2017) Enabling evidence based continuous improvement: The target architecture – Connected care settings and improving patient experience. Available at https://medconfidential.org/wp-content/uploads/2017/09/2017-07-13-Target-Architecture.pdf (accessed 21 May 2021).

MELD, University of Southampton (2021) Research project: Developing a multidisciplinary ecosystem to study lifecourse determinants of complex mid-life multimorbidity using artificial intelligence (MELD). Faculty of Medicine. Available at https://www.southampton.ac.uk/medicine/academic_units/projects/meld.page (accessed 21 May 2021).

Miller FA, **Patton SJ**, **Dobrow M and Berta W** (2018) Public involvement in health research systems: A governance framework. *Health Research Policy and Systems 16*, 79. https://doi.org/10.1186/s12961-018-0352-7

Moses B and Desai K (2020). Data governance is broken. Information Week. Available at https://informationweek.com/big-data/data-governance-is-broken-/a/d-id/1339635 (accessed 21 May 2021).

Muller SHA, **Kalkman S**, **van Thiel GJMW**, **Mostert M and van Delden JJM** (2021) The social licence for data-intensive health research: Towards co-creation, public value and trust. *BMC Medical Ethics 22*, 110. https://doi.org/10.1186/s12910-021-00677-5

Multidisciplinary Ecosystem to study Lifecourse Determinants of Complex Mid-life Multimorbidity using Artificial Intelligence (MELD) (2020) Project proposal. University of Southampton. Internal document.

National Cyber Security Centre (n.d.) UK Cyber Essentials Plus. Available at https://www.ncsc.gov.uk/cyberessentials/overview (accessed 20 May 2021).

NHS (2019) The NHS long term plan. V1.2. Available at https://www.longtermplan.nhs.uk/wp-content/uploads/2019/08/nhs-long-term-plan-version-1.2.pdf (accessed 21 May 2021).

NHS (n.d.) Placed based approaches to reducing health inequalities. Available at https://www.england.nhs.uk/ltphimenu/placed-based-approaches-to-reducing-health-inequalities/ (accessed 21 May 2021).

NHS Data Security and Protection Toolkit (2021) Available at https://www.dsptoolkit.nhs.uk/ (accessed 21 May 2021).

NHS Digital (n.d.) Data Access Request Service (DARS). Available at https://digital.nhs.uk/services/data-access-request-service-dars (accessed 20 May 2021).

NHS Health Research Authority (HRA) (2019) Prepare study documentation. Last updated: 17 July 2019. Available at https://www.hra.nhs.uk/planning-and-improving-research/research-planning/prepare-study-documentation/ (accessed 14 December 2021).

https://doi.org/10.1017/dap.2022.1 Published online by Cambridge University Press

NHS Health Research Authority (HRA) (2021) HRA approval. Last updated: 22 November 2021. Available at https://www.hra.nhs.uk/approvals-amendments/what-approvals-do-i-need/hra-approval/ (accessed 14 December 2021).

Northern Health Science Alliance (NSHA) (2020) Connected health cities: Impact report 2016–2020. Available at https://www.thenhsa.co.uk/app/uploads/2020/10/CHC-full-impact-report.pdf (accessed 21 May 2021).

O'Hara K (2019) Data trusts: Ethics, architecture and governance for trustworthy data stewardship. Web Science Institute (WSI) White Paper #1. Available at https://www.southampton.ac.uk/wsi/enterprise-and-impact/white-papers.page (accessed 20 May 2021).

O'Hara K (2021) From internal discussions with authors on the notion of fiduciary ethical virtues and *datatrust* services.

Ocloo J and Matthews R (2016) From tokenism to empowerment: Progressing patient and public involvement in healthcare improvement. *BMJ Quality & Safety 25*(8), 626–632. http://doi.org/10.1136/bmjqs-2015-004839

Oswald M (2013) Something bad might happen: Lawyers, anonymization and risk. *XRDS 20*(1), 22–26. https://doi.org/10.1145/2508970.

OWASP (2021) OWASP top ten. Available at https://owasp.org/www-project-top-ten/ (accessed 20 May 2021).

Pozen DE (2005) The Mosaic theory, national security, and the freedom of information act. *Yale Law Journal 115*, 628–679. Available at SSRN https://ssrn.com/abstract=820326 (accessed 20 May 2021).

Public Health England (2017) Reducing health inequalities: System, scale and sustainability. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/731682/Reducing_health_inequalities_system_scale_and_sustainability.pdf (accessed 21 May 2021).

Public Health Research Data Forum (2015). Enabling data linkage to maximise the value of public health research data: Full report. Available at https://cms.wellcome.org/sites/default/files/enabling-data-linkage-to-maximise-value-of-public-health-research-data-phrdf-mar15.pdf (accessed 21 May 2021).

Research Data Alliance (RDA) COVID-19 Working Group (2020) RDA COVID-19; Recommendations and guidelines on data sharing, final release 30 June 2020. https://doi.org/10.15497/rda00052.

Rieke N, **Hancox J**, **Li W**, **Milletari F**, **Roth HR**, **Albarqouni S**, **Bakas S**, **Galtier MN**, **Landman BA**, **Maier-Hein K**, **Ourselin S**, **Sheller M**, **Summers RM**, **Trask A**, **Xu D**, **Baust M and Cardoso MJ** (2020) The future of digital health with federated learning. *NPJ Digital Medicine 3*, 119. https://doi.org/10.1038/s41746-020-00323-1

Rooney D, **Leach J and Ashworth P** (2014) Doing the social in social licence. *Social Epistemology 28*(3–4), 209–218. https://doi.org/10.1080/02691728.2014.922644

Sadana R and Harper S (2011) Data systems linking social determinants of health with health outcomes: Advancing public goods to support research and evidence-based policy and programs. *Public Health Reports 126*(3), 6–13. https://doi.org/10.1177/00333549111260S302

SAIL (2021) Databank. Available at https://saildatabank.com/ (accessed 21 May 2021).

Scott K (2018). Data for Public Benefit: Balancing the risks and benefits of data sharing. Report Co-authored by Understanding Patient Data, Involve and Carnegie UK Trust. Contributors: Burall S, Perrin N, Shelton P, White D, Irvine G and Grant A. Available at https://www.involve.org.uk/sites/default/files/field/attachemnt/Data%20for%20Public%20Benefit%20Report_0.pdf (accessed 24 May 2021).

Sharon T and Lucivero F (2019) Introduction to the special theme: the expansion of the health data ecosystem—Rethinking data ethics and governance. *Big Data & Society 6*, 1–5. https://doi.org/10.1177/2053951719852969

Smart Dubai and Nesta (2020) Data sharing toolkit: Approaches, guidance and resources to unlock the value of data. Available at https://www.nesta.org.uk/toolkit/data-sharing-toolkit/ (accessed 4 June 2021).

Sohail O, **Sharma P and Ciric B** (2018) Data governance for next-generation platforms. Deloitte. Available at https://www2.deloitte.com/us/en/pages/technology/articles/data-governance-next-gen-platforms.html (accessed 20 May 2021).

Spinney L (2021). Hospitals without walls: The future of healthcare. The Guardian. Available at https://www.theguardian.com/society/2021/jan/02/hospitals-without-walls-the-future-of-digital-healthcare (accessed 21 May 2021).

Stalla-Bourdillon S, **Carmichael L and Wintour A** (2021) Fostering trustworthy data sharing: Establishing data foundations in practice. *Data & Policy 3*, e4. https://doi.org/10.1017/dap.2020.24

Stalla-Bourdillon S, **Wintour A and Carmichael L** (2019) Building Trust through Data Foundations: A Call for a Data Governance Model to Support Trustworthy Data Sharing. Web Science Institute (WSI) White Paper #2. Available at https://www.southampton.ac.uk/wsi/enterprise-andimpact/white-papers.page (accessed 21 May 2021).

Surridge M, **Correndo G**, **Meacham K**, **Papay J**, **Phillips SC**, **Wiegand S and Wilkinson T** (2018) Trust modelling in 5G mobile networks. In *Proceedings of the 2018 Workshop on Security in Softwarized Networks: Prospects and Challenges (SecSoN '18)*. Workshop Co-Chairs: Benson T, Bisson P, Pries R and Zinner T. New York, NY: ACM, pp. 14–19. https://doi.org/10.1145/3229616.3229621

Surridge M, **Meacham K**, **Papay J**, **Phillips SC**, **Pickering JB**, **Shafiee A and Wilkinson T** (2019) Modelling compliance threats and security analysis of cross border health data exchange. In Attiogbé C, Ferrarotti F and Maabout S (eds), *New Trends in Model and Data Engineering. MEDI 2019. Communications in Computer and Information Science*, Vol. *1085*. Cham: Springer. https://doi.org/10.1007/978-3-030-32213-7_14

Taylor S, **Surridge M and Pickering B** (2020) Regulatory compliance modelling using risk management techniques. Available at SSRN http://doi.org/10.2139/ssrn.3716778

The Toronto Declaration (2018) Protecting the right to equality and non-discrimination in machine learning systems. Amnesty International and AccessNow (eds). Available at https://www.torontodeclaration.org/wp-content/uploads/2019/12/Toronto_Declaration_English.pdf (accessed 21 May 2021).

Thompson Reuters: Practical Law (n.d.) Fiduciary duties and fiduciary. Glossary. Available at https://uk.practicallaw.thomsonreuters.com/1-107-5744?transitionType=Default&contextData=(sc.Default)&firstPage=true (accessed 30 November 2021).

Triggle N (2021). Is COVID at risk of becoming a disease of the poor? *BBC News,* February 2021. Available at https://www.bbc.co.uk/news/health-56162075 (accessed 21 May 2021).

UK Data Service (1970) 1970 British Cohort Study (BCS70). Available at beta.ukdataservice.ac.uk/datacatalogue/series/series?id=200001 (accessed 20 May 2021).

UK Data Service (n.d.) Regulating access to data: 5 Safes. Available at https://www.ukdataservice.ac.uk/manage-data/legal-ethical/access-control/five-safes (accessed 20 May 2021).

UK Department of Health and Social Care (2021) A guide to good practice for digital and data-driven health technologies. Available at https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology/initial-code-of-conduct-for-data-driven-health-and-care-technology (accessed 21 May 2021).

UK Government Chief Scientific Adviser (2016) Distributed ledger technology: Beyond block chain. Government Office for Science. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf (accessed 21 May 2021).

UK Health Data Research Alliance (UKHDRA) (2020) Trusted Research Environments (TRE): A strategy to build public trust and meet changing health data science needs. Green Paper v2.0 dated 21 July 2020. Available at https://ukhealthdata.org/wp-content/uploads/2020/07/200723-Alliance-Board_Paper-E_TRE-Green-Paper.pdf (accessed 21 May 2021).

UK Health Data Research Alliance (UKHDRA) (n.d.) Innovation Gateway. Available at https://www.healthdatagateway.org/ (accessed 21 May 2021).

Understanding Patient Data and Ada Lovelace Institute (2020) Foundations of fairness: Where next for NHS health data partnerships. Available at https://understandingpatientdata.org.uk/sites/default/files/2020-03/Foundations%20of%20Fairness%20-%20Summary%20and%20Analysis.pdf (accessed 21 May 2021).

University of Southampton (2021) Social impact lab. Available at https://www.southampton.ac.uk/silab/index.page (accessed 20 May 2021).

Varshney S (2020). A progressive approach to data governance. *Forbes.* Available at https://www.forbes.com/sites/forbestechcouncil/2020/11/03/a-progressive-approach-to-data-governance/ (accessed 20 May 2021).

Wessex Care Records (2021) Available at https://www.wessexcarerecords.org.uk/ (accessed 20 May 2021).

Winter JS and Davidson E (2019) Big data governance of personal health information and challenges to contextual integrity. *The Information Society 35*(1), 36–51. https://doi.org/10.1080/01972243.2018.1542648

World Health Organization (n.d.) social determinants of health. Available at https://www.who.int/health-topics/social-determinants-of-health (accessed 20 May 2021).

Young M, **Rodriguez L**, **Keller E**, **Sun F**, **Sa B**, **Whittington J and Howe B** (2019) Beyond open vs. closed: Balancing individual privacy and public accountability in data sharing. In *Proceedings of the Conference on Fairness, Accountability, and Transparency (FAT* '19)*. General Co-Chairs: Boyd, D and Morgenstern J. Program Co-Chairs: Chouldechova A and Diaz F. New York: Association for Computing Machinery (ACM), pp. 191–200. https://doi.org/10.1145/3287560.3287577

Cite this article: Boniface M, Carmichael L, Hall W, Pickering B, Stalla-Bourdillon S and Taylor S (2022). The Social Data Foundation model: Facilitating health and social care transformation through *datatrust services*. *Data & Policy*, 4: e6. doi:10.1017/dap.2022.1

https://doi.org/10.1017/dap.2022.1 Published online by Cambridge University Press