

The Social Data Foundation Model: Facilitating Health and Social Care Transformation through *Datatrust Services*

Pre-print | Research Article | v0.1 | 7 June 2021

Prof Michael Boniface – <https://orcid.org/0000-0002-9281-6095>

Dr Laura Carmichael* – <https://orcid.org/0000-0001-9391-1310>

Prof Dame Wendy Hall – <https://orcid.org/0000-0003-4327-7811>

Dr Brian Pickering – <https://orcid.org/0000-0002-6815-2938>

Prof Sophie Stalla-Bourdillon

Dr Steve Taylor – <https://orcid.org/0000-0002-9937-1762>

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

Interdisciplinary Centre for Law, Internet and Culture (iCLIC) | IT Innovation | Web Science Institute (WSI)

University of Southampton

Abstract

Turning the wealth of health and social data into insights to promote better public health, whilst enabling more effective personalised 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, involves 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 re-identification risk over time, and the challenge of establishing and maintaining a social licence. *Datatrust services* are a socio-technical 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’ (TRE). In this paper, we explore: the requirements for *datatrust services*; a proposed implementation – the Social Data Foundation (SDF); and, an illustrative test case. Moving forward, such an approach would help incentivise, 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.

Keywords

Healthcare and Social Care; Data Governance Models; *Datatrust Services*; Data Stewardship; Data Institutions

Policy Significance Statement

Turning the wealth of health and social data into insights for better public health and personalised 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 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.

The Social Data Foundation Model: Facilitating Health and Social Care Transformation through *Datatrust Services*

Boniface, M., Carmichael, L., Hall, W., Pickering, B., Stalla-Bourdillon, S. & Taylor, S.

1. Introduction

Social determinants of health significantly affect individual well-being and health inequalities (Marmot et al., 2020; Public Health England, 2017; Sadana & Harper, 2011). The World Health Organization (n.d.) describes ‘social determinants of health’ as “non-medical factors that influence health outcomes” such as “education”, “working life conditions”, “early childhood development”, and “social-inclusion and non-discrimination”. The global COVID-19 pandemic highlights how “disparities in social determinants of health” (Burström & 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 & Szeffler, 2020; Burström & Tao, 2020; Triggler, 2021).

Social determinants of health can be acquired from diverse data sources – e.g., wearables, digital health platforms, social media, environment monitoring – many beyond the conventional boundaries of health and social care (e.g., Sharon & Lucivero, 2019). The “safe” linkage (UK Data Service, n.d., b; 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 bringing together with other more conventional data types (e.g., electronic healthcare records, public health statistics, 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 personalised 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 incentivising and accelerating sharing of regulated data and any associated outputs across relevant stakeholders (e.g., healthcare or social care providers, researchers, public health authorities, 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

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 E.g., via public interventions, targeted health and well-being campaigns.

³ E.g., through personalised medicine, increased patient and/or service user empowerment, 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 non-clinical purposes) related to health and social care systems transformation. Data users can request access to data e.g., via applications to

pandemic (e.g., Research Data Alliance (RDA) Covid-19 Working Group, 2020). Trustworthy data governance is essential not only to ensure data providers and users can fulfil their regulatory obligations, but also to maintain public confidence and engagement (Geissbuhler et al., 2013; Stalla-Bourdillon et al., 2021). Advanced data governance⁵ models are therefore required that can foster a “social licence” (Carter et al., 2015; Jones & Ford, 2018, O’Hara 2019) and which can handle increasing data volumes and complexity safely (e.g., Sohail et al., 2018; Winter & 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 socio-technical model for good data governance, sensitive to the needs of all stakeholders, and allied with advances in dynamic and secure federated research environments. In this paper, we demonstrate why the SDF model is well equipped to support health and social care transformation for individual and community benefit,⁷ boost open science, and generate insights for multiple stakeholders. We validate our SDF model through its application to a test case centred 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).

2. ‘Trusted Research Environments’ (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 “trusted research environments” (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),⁸ 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).

Data Access Request Service (DARS) provided by NHS Digital, individual NHS trusts and foundations, and local health and care records programmes (e.g., Wessex Care Records).

⁵ Whilst there is no universal definition of the term ‘data governance’, Janssen et al. (2020) provide a useful description of this term in a multi-organisational 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 & Nesta (2019) 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: “organisations whose purpose involves stewarding data on behalf of others, often towards public, educational or charitable aims” (Dodds et al., 2020).

⁷ E.g., alignment with the CARE principles (2018).

⁸ Trusted third party intermediaries continue to play a crucial role in facilitating data linkage for public health research and innovation – such as, SAIL (Jones et al., 2014) for linkage of specified anonymised datasets, and UK Health Data Research Alliance (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 eleven 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; and Data Linkage Western Australia.

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 re-used. Generated outputs from any data linkage activities (e.g., containers, derived data, images, notebooks, publications, software) are often not adequately disclosed (UKHDRA, 2020), making it more difficult to effectively mitigate the risk of re-identification, 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 utility⁹ (e.g., data providers may share only aggregated data where de-identified 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 licence for specific health and social care research and innovation activities.

2.2. Upholding a Social Licence

A social licence 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 licence is supported by its perceived trustworthiness (which can be expressed in terms of benevolence, integrity and ability (Mayer, 1995)) towards the society it intends to serve. For instance, aligning ethical oversight with the CARE principles (2018) brings to centre stage the need to ensure equanimity across the data lifecycle. The UKHDRA (2020) describes the principal rationale 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) outline TRUST principles for data infrastructures (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 vulnerable. Similarly, the UK Data Ethics Framework (Central Digital & 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 emphasise respect for individual rights within the context of potential community benefit, accountability, and transparency. Beyond this, though, for stakeholders to agree a social licence, it must be clear that the rights and expectations of individuals and the communities they represent should be upheld.

⁹ While strong de-identification of data is vital to protect the rights of (groups of) individuals, de-identification can lower the utility of data. The definition of anonymised data is provided by GDPR 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 anonymised data. As a matter of principle, two different processes can lead to anonymised 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 de-identification (i.e., data remains at the individual level). In both cases, data and context controls should be combined to guarantee that re-identification risk is “remote” over time (ICO, 2012).

2.3. Bringing Citizens Back to Centre Stage

To promote social licence 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 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 & 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 & Matthews, 2016) – especially where healthcare data are (re)used by third parties (Understanding Patient Data & 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 are 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 co-design and co-evaluation 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, 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 & 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
- (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 whilst appreciating potential impacts of community size. A diameter of trust cannot be predicated solely on demographics (e.g., geographic scope, 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 TRE data governance model must be progressive, learning iteratively, integrating new best practice without undue delay, as well as remaining compliant with the changing legal landscape. Best practice may be both organisational (e.g., the adoption of codes of conduct, 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 learnt 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”.

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

2.6. Adhering to the “Five Safes Plus One”

Best practice for TREs is centred on the ‘Five Safes Framework’ (UKHDRA, 2020). The framework was devised in 2003 by 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 & 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 authorised 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 organisational infrastructure to ensure all data related-activities are undertaken securely and safely.

- **“Safe data”**: all other ‘safes’ are adhered to; data are de-identified appropriately before re-usage via the TRE, and remain appropriately de-identified 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 authorisation.
- **“Safe return”**: to ensure that recombination of TRE outputs with other data at the “the clinical setting that originated the data” – which may re-identify data subjects – is only undertaken if permitted and consented by the data subjects concerned. (UK Health Data Research Alliance, 2020).¹⁰

A collaborative health and social care data sharing scheme must also fulfil essential data governance requirements for ethics (e.g., institutional approval, Integrated Research Application System (IRAS) approval), legal-compliance (e.g., data protection, confidentiality, contracts, intellectual property), and cyber-security, (e.g., UK Cyber Essentials Plus, ISO27001, NHS Data Security and Protection Toolkit).¹¹

3. The Social Data Foundation (SDF) Model

Models of safe and high-quality data linkage from multiple agencies necessitate a high-level of interdisciplinarity (Jacobs & Popma, 2019) wider than the conventional boundaries of medicine and social care (Ford et al., 2019; Sharon & Lucivero, 2019). To address this, the SDF model has adopted a socio-technical approach¹² 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 multi-stakeholder health and social care data needs to be aggregated at different levels (e.g., locally, regionally and nationally), the SDF offers a localised hub for data-intensive research and innovation facilitating multi-party 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, whilst offering national exemplars of health system solutions.

In order for the SDF to acquire and maintain a social licence, 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.¹³ 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

¹⁰ 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 re-identify information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data”.

¹¹ For a non-exhaustive list of data governance requirements see Boniface et al. (2020).

¹² Note that the SDF initiative brings together a multi-disciplinary 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.

¹³ 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).

generated project outputs; and, demonstrated positive health and social care transformation impacts for certain stakeholder groups.

Whilst 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 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 anonymisation, 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.

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 licence.

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).¹⁴ However, the relationship is *not* a fiduciary one in the full *legal* sense, 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 organisations, 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 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.

¹⁴ 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*.

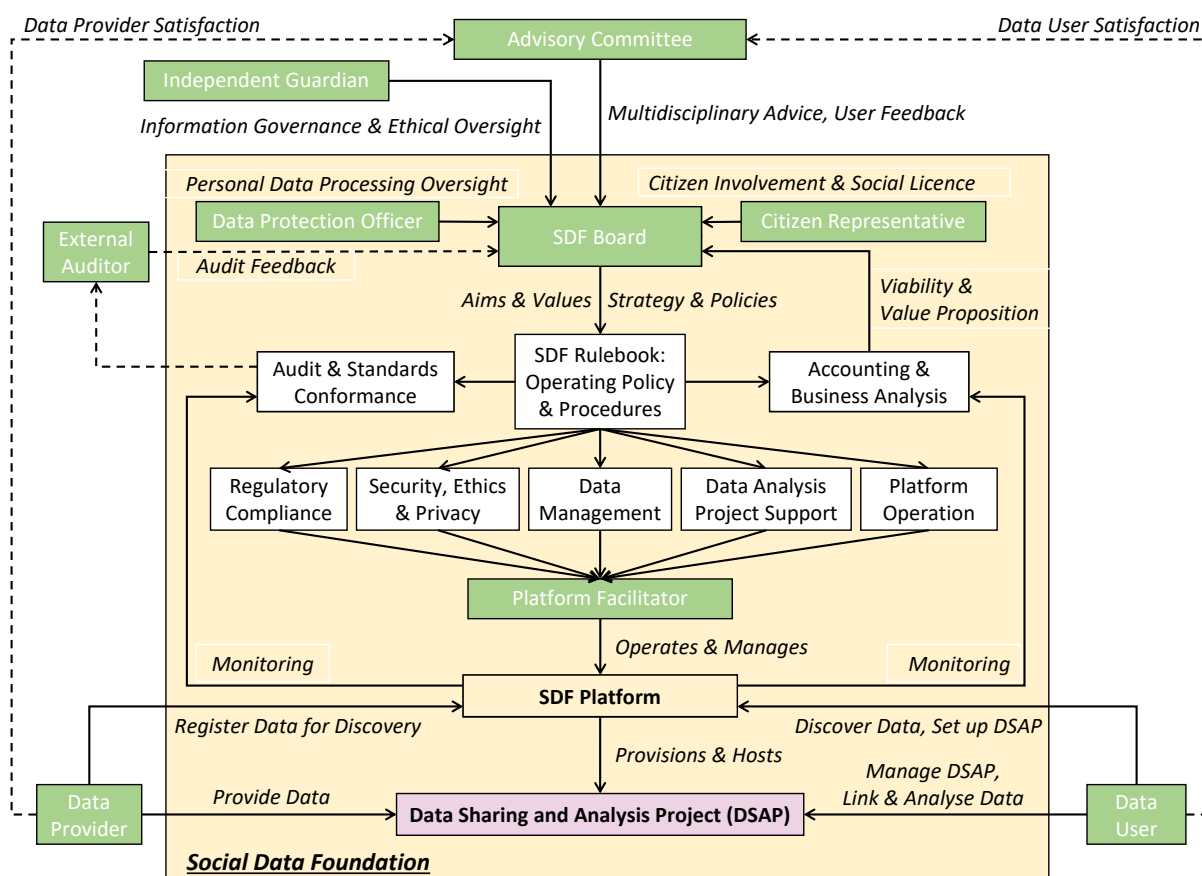


Figure 1: SDF Governance Structure

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, 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 licence. In particular, Citizen Representatives shall create, implement and manage a framework for citizen participation and engagement activities, where citizens can co-create and participate in health and social care systems transformation as well as exercise their data-related rights.¹⁵
- Data Provider.** An entity is the owner or rights holder of data that is either discoverable via the Platform, hosted by the Platform, or utilised in DSAPs. The Data Provider is typically an organisational 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 who 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 Note that the SDF appeared as a case study in a report on “Exploring legal mechanisms for data stewardship” published by Ada Lovelace & the UK AI Council (2021).

- **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 analysing datasets.
- **Data Protection Officer (DPO).** A standard role (whose appointment in some instances is mandatory under the GDPR) for organisations who 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 re-identification 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 back 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 re-identification when project results are reintegrated with source data, whether re-identification 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 realise the highest standards of excellence for data governance in accordance with applicable policies and processes that govern the operation of the SDF Platform. In particular, the Independent Guardian shall: (i) help set up a risk management framework for data sharing; (ii) assess the proposed data use cases in accordance with this risk management framework; and, (iii) audit and monitor day-to-day all 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, Users, and Citizens. Feedback from Data Providers and 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 is a central body of the Governance of the SDF, in that it 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” – i.e., 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: Examples of Key Standardised Processes for all DSAPs

Key Standardised Process for all ‘Data Sharing and Analysis Projects’ (DSAPs)	Relation to the ‘Five Safes Plus One’:
<p>a. The SDF DSAP Approval Process</p> <p>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.</p>	<p>“Safe people”; “Safe projects”</p>
<p>b. The SDF DSAP Container Process</p> <p>DSAPs must be secure and isolated from other projects and data.</p>	<p>“Safe setting”</p>
<p>c. The SDF DSAP Default Access Policy</p> <p>There must be a default access policy that prevents unauthorised data export or download from the secure environment.</p>	<p>“Safe outputs”</p>
<p>d. The SDF DSAP Audit Trail Process</p> <p>DSAPs must have their activities recorded for audit purposes in a non-repudiable way; a project audit record is shared between the Project Manager, the relevant Data Provider(s), and the SDF Platform</p>	<p>“Safe setting”</p>
<p>e. The SDF DSAP Functional Anonymisation Process</p> <p>DSAPs must process data legally, ethically, and securely – in accordance with all applicable data sharing licences and/or agreements, ethics approvals, and all other necessary requirements. The SDF must practise “functional anonymisation”, which is defined by Elliot et al. (2018) as</p> <p style="padding-left: 40px;">“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”</p>	<p>“Safe data”; “safe projects”; “safe setting”</p>

3.2. Datatrust Services

Datatrust services are a socio-technical evolution that advances databases and data management systems towards 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 multi-sided service platform (the SDF Platform), which creates value through linked data interactions between Data Providers and Data Users, whilst implementing the necessary management and governance arrangements. We now describe the specific functionalities of our *datatrust service*

platform recognising 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 (on a subsequent page) depicts a *datatrust service platform* embedded into the ‘SDF Governance Model’ (section 3.1). Some key features of the *datatrust service platform* are as follows:

‘Value & Proportionality’

These services are necessary to ensure “value and proportionality” within the defined remit of the SDF for stakeholder approval (i.e., maintaining a social licence) and ethical oversight. These services provide oversight for the lifecycle of DSAPs through stages of request, orchestration, knowledge discovery, and artefact release.

‘Purpose’

These services are required so that the purpose of DSAPs are specified in templates, which 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 anonymisation environments dynamically with repeatability.

‘Data Configuration’ and ‘Environment Configuration’

These services give rise to functional anonymisation – the property of functional anonymisation is important and concerned with addressing risk of re-identification by controlling the data and its environment:

“... 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, [and] infrastructure”. (Elliot et al., 2018).

Interpreting these four elements 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 re-identification 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 – e.g., for ethical approval, stakeholder acceptance, policy enforcement through contracts, licences 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 centres (e.g., public cloud, private cloud, edge). *Datatrust services* are deployed as a cloud tenant, and utilise 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 to enable NHS health data processing). In addition, *datatrust services* are operated within a cyber security risk assessment and mitigation process to guard against cyber threats and attacks – guided by ISO 27005, and compliant with ISO 27001 risk management.

Once a DSAP is deployed, Data Users can access data services that operate on the datasets within the DSAP to produce artefacts 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 licence, and updated data services available for deployment in new DSAPs.

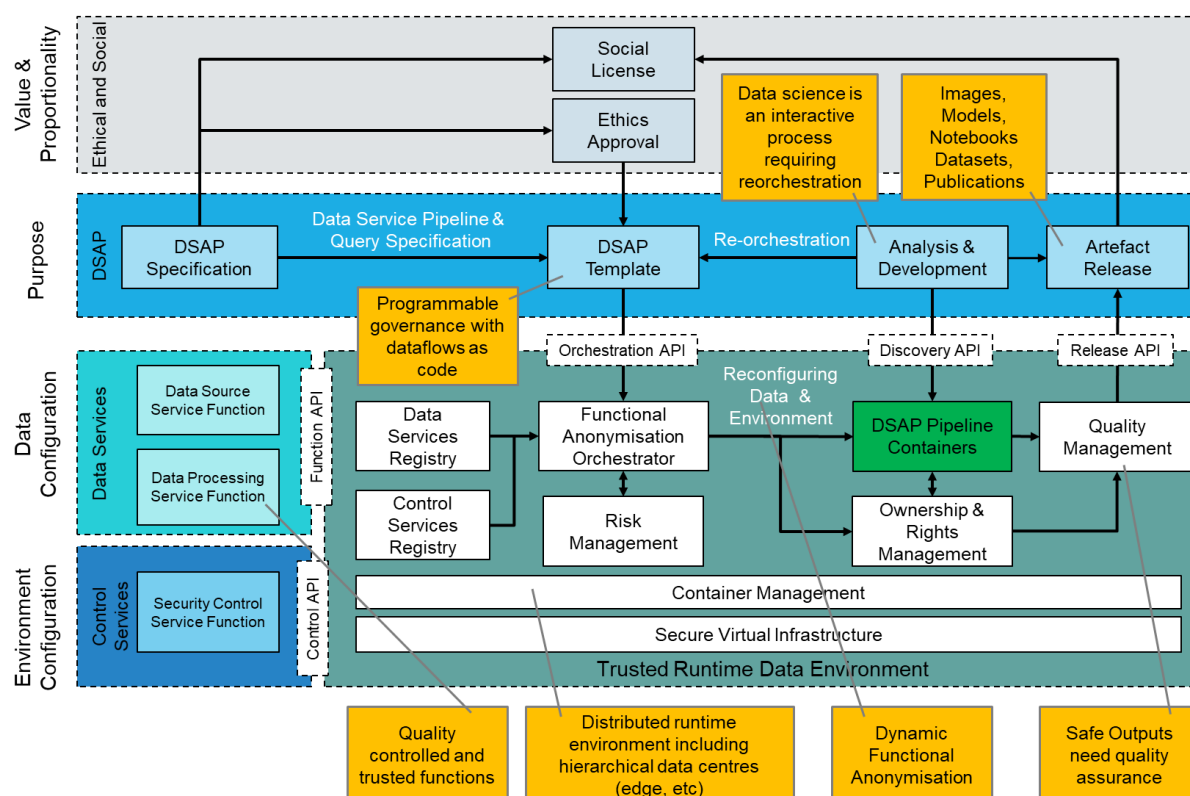


Figure 2: A Datatrust Service Platform

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: (i) data de-identification; (ii) data cleaning; (iii) data quality assurance; (iv) data consistency assurance (e.g., ensuring pseudonymised identifiers are consistent across datasets); and (v) data harmonisation and compatibility assurance (e.g., normalising data fields across heterogeneous data sets generated by different software). The use of standardised metadata, including provenance records, is important to make it possible to interpret and link datasets. HL7 FHIR (Bender

& 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 harmonisation remaining a topic of significant research.

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

“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 tokenised link identifiers (Jones et al., 2014), whilst 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 licence and risk management are key characteristics of *datatrust services*. In the following sub-sections, we describe four important aspects of *datatrust service* functionality in more detail: functional anonymisation, specification of data and dataflows, compliance decision support, and ownership and rights management.

3.2.3 ‘Functional Anonymisation Orchestrator’ (FOA)

What is the FOA?

The FOA is the *datatrust service* for functional anonymisation – 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 FOA interfaces with a registry of pre-approved, trusted data service functions and environment controls, as well as the Risk Management (RM) 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 ensure that *datatrust services* offer the property of functional anonymisation – and therefore works to address its key elements, as cited by Elliot et al. (2018).

3.2.4 ‘DSAP Template’

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’ (DPIAs).

How does it work?

The FAO 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 standardisation of templates and APIs will be essential for interoperability between *datatrust services* governing health and social care data.

DSAP Template	Baseline	Description
Platform Hosted		Data are uploaded to the Platform from a Data Provider and then subsequently imported and linked within a DSAP. <i>Applies to situations where data are hosted by the Platform only.</i>
Project Hosted		Data are uploaded and linked within a DSAP from one or more Data Providers. <i>Applies to situations where data are made discoverable via the Platform, but are not hosted by the Platform.</i>
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. <i>Applies to situations where Data Providers wish to maximise control over their datasets.</i>
Hybrid Hosted and Query		Data is linked in some combination of Platform Hosted, Project Hosted and Federated Query

Table 2: Data Sharing and Analysis Project Template Types

Templates are technical in nature and therefore a predefined set of baseline templates are defined for different project types, as outlined in Table 2. The 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 ‘Risk Management’ (RM)

What is the RM?

The RM is the *datatrust service* for regulatory compliance decision support for DSAP pipelines – and utilises an asset-based risk modelling approach following ISO 27001; initially based on cyber security.

How does it work?

Risk is explicitly defined in relation to *threats* upon *assets*. Assets are tangible and non-tangible items of value – whilst datasets are core assets of interest, other assets include software, data, machinery, services, people, and reputation. Assets may be attacked by threats, which causes *misbehaviour* in the asset (i.e., unwanted, erroneous or dangerous behaviour). The *risk* to the asset is the severity of the misbehaviour combined with the likelihood of the threat. *Controls* may be applied to the asset to reduce the likelihood of the threat occurring.

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 RM approach

therefore include cyber security, such as those associated with OWASP Top Ten (2021), or compliance threats due to failures in regulatory or licensing compliance.

The RM approach detects cyber security or regulatory compliance threats based on a specified DSAP template, and provides recommendations for controls (mitigating strategies) to block a compliance threat sufficiently to satisfy a regulatory requirement. Whilst 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 a potential risk – re-identification

A key risk to be mitigated is the potential for re-identification that can arise through data sharing, usage and re-usage in DSAPs. Oswald (2013) defines the risk of re-identification 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” – i.e., 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 RM 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 pseudonymisation, k-anonymisation) 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, aggregation). The RM provides risk assessment to the FAO 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 de-identify data.

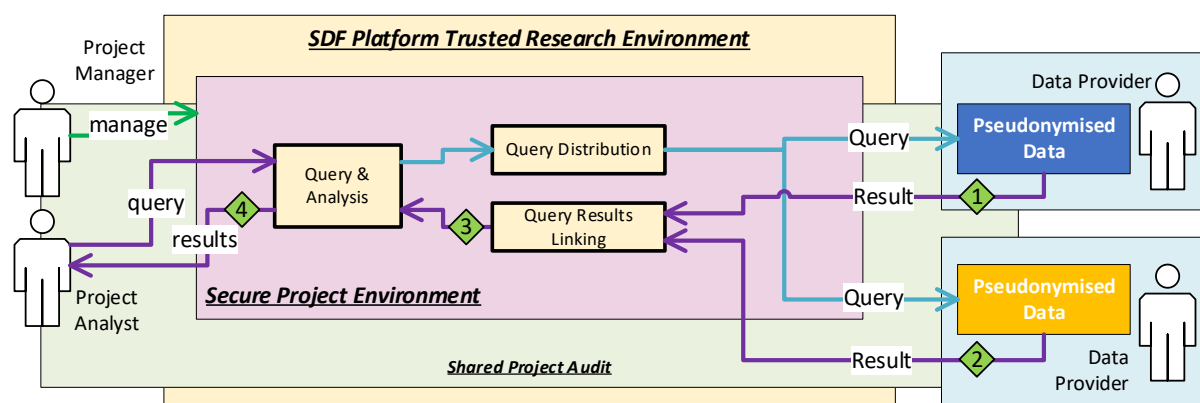


Figure 3: Re-identification risk assessment for distributed query

As an example, Figure 3 shows the risk assessment points for the ‘Federated Query DSAP Template’. Policy enforcement is dynamic with checkpoints 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. Checkpoint 3) occurs after the result fragments are linked, and checkpoint 4) occurs after any analysis processing on the linked result. A key difference between the Platform Hosted and Federated Query scenarios is that some of the re-identification risk checking are distributed to Data Provider whereas in the Platform Hosted scenario, all checking is undertaken by the operator of the Platform. This ability to check for re-identification risk on a per-query basis at Data Provider premises 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 non-repudiable way. This *datatrust service* therefore ensures that all permitted stakeholders for a specified DSAP – e.g., 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?

(1) Distributed Ledger Technology (DLT)

To provide such ‘Shared Project Audit Distributed Ledgers’, the SDF employs DLT – 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).

DLT 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 behaviour.

(2) Smart Contracts

To ensure compliance with all specified data sharing agreements and/or licences applicable to a DSAP, the ‘Ownership and Rights Management’ *datatrust service* also employs Smart Contracts technology. Smart Contracts are related to DLT – 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 ‘licence 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.

E.g., a Smart Contract can implement data linking using pseudonymised 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 licence 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 licence terms therefore can be enforced at the point of execution by the Data Analyst. This automated enforcement prevents Data Analysts executing operations that are inconsistent with the licence terms of Data Providers.

E.g., if one Data Provider prohibits pseudonymised linking, their dataset will not be available to a Smart Contract implementing pseudonymised 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 DLT), 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 licence terms to be enforced. Whilst 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 licence terms frequently used across many types of DSAPs.

4. Validation of the SDF Model

To validate the SDF model we now analyse 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 (NIHR) – 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 personalised 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 analysing the social determinants of health using complex linked social and health datasets. MELD is part of a multi-disciplinary 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 – e.g., derived data, AI/ML models, tooling.

4.2. MELD 1.0: Initial Project

The first phase of MELD brings together a multi-disciplinary team – including researchers from medicine, social science, and computer science – and patient and public involvement (PPI) representatives to explore lifecourse 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, n.d., a) 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 (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 organisations 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 have carried out a DPIA.

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 characterised; 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, 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 – e.g., 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 whilst helping stakeholders manage associated risks efficiently. The stakeholders include the Health Research Authority (HRA), two data providers (NHS for CHIA and the UK Data Service for BCS70), the MELD Principal Investigator (PI), who takes the role of Project Manager, and Data Analysts working on the project.

Initially, the MELD PI must establish the necessary research ethics approvals, data access rights and resources to undertake research necessary to delegate rights to Data Analysts with the team. In the UK, the NHS HRA provides overall authority for health and social care research aiming to

“protect and promote the interests of patients and the public in health and social care research”. (NHS HRA, n.d.).

NHS HRA approval requires a PI to provide detailed study information along with supporting documents such as ‘Organisation Information Document’, ‘Schedule of Events’ and ‘Sponsors Insurance’ provided by the PI’s host organisation following local approval. Institutional and national governance processes for approval requests require similar information but there is little standardisation between processes and document structures, whilst 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, risk management can be directly embedded into research processes and 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 standardisation will be required.

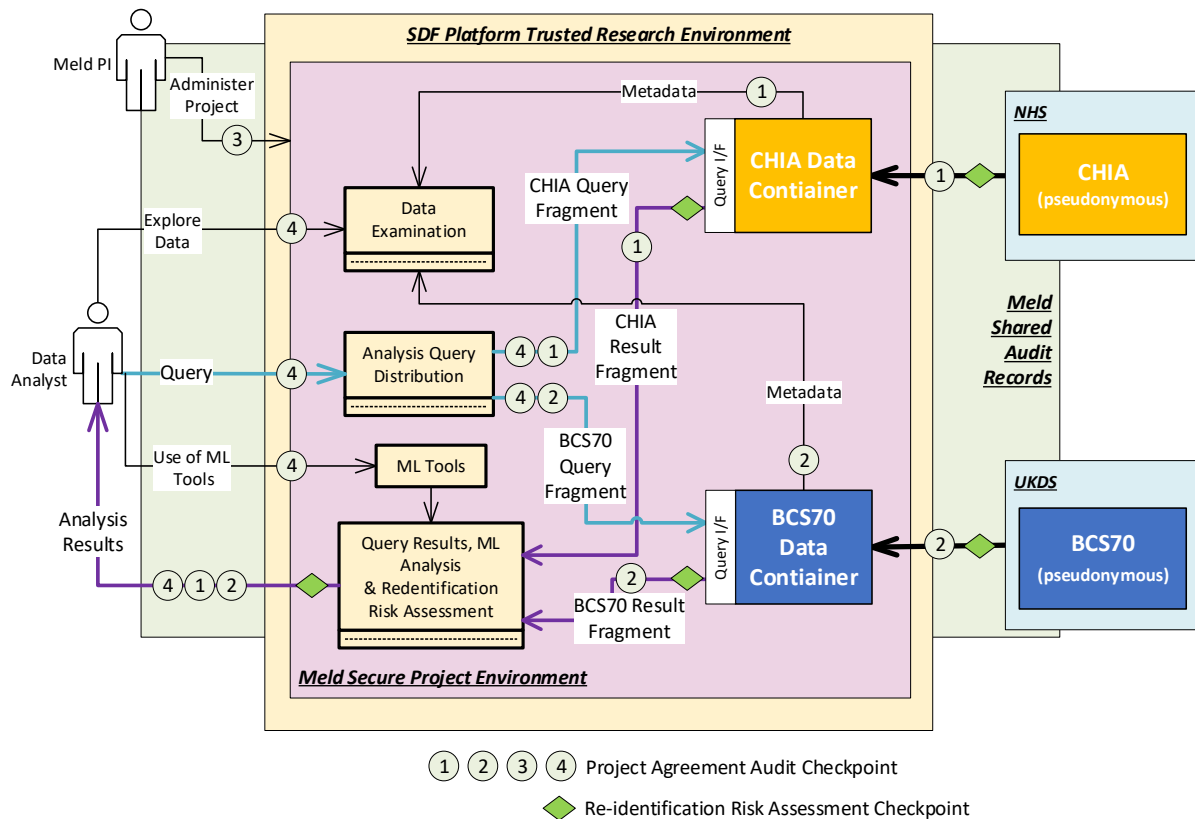


Figure 4: MELD within the datatrust service platform

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

- (1) The MELD PI requests a DSAP, completes a DSAP template with data configuration (inclusion, exclusion, 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 MELD PI 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 MELD PI makes an agreement with SDF for a DSAP (denoted by the green circle 3 in Figure 4).
- (5) The SDF creates a DSAP for MELD. The project (pink box in Figure 4) is a secure environment isolated from other projects and access for Data Analysts is specified by the MELD PI and enforced by the Platform.
- (6) The MELD PI acquires agreements and/or licences from data providers, which will come with terms of use that must be respected (denoted by the green circles 1 and 2 respectively in Figure 4). The MELD PI names the SDF as their TRE in agreement with Data Providers.
- (7) The datasets are acquired from the Data Providers by the SDF (as the named delegate by PI) – and are loaded into the MELD DSAP.
- (8) The MELD PI authors the MELD Data Usage Policy (denoted by green circle 4 in Figure 4), which must be consistent with the licences and/or agreements between the MELD PI and the Data Providers (green circles 1 and 2 in Figure 4).
- (9) The MELD PI appoints analysts, who must agree to the MELD Data Usage Policy.
- (10) The MELD PI grants access to the MELD DSAP for each approved 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) The MELD Analyst explores dataset metadata limited by those defined in the DSAP specification.
- (2) The MELD Analyst formulates queries, which may be on an individual dataset or inferences between datasets. Queries must be consistent with:
 - a. Data Usage Terms of the DSAP; and
 - b. Approvals (IRAS for CHIA; UK Data Service End User Agreement for BCS70).
- (3) The MELD Analyst runs queries and uses ML tools to analyse the resultant data. Depending on the query from the Analyst, the results may be from one dataset or both datasets linked by common attributes. 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.

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 localised solutions with national leadership'. We now explore each proposed benefit – and how it can be realised for the MELD project:

4.4.1 Empowerment of Citizens

Given the depth of data required to understand lifestyle behaviours, socio-economic factors, and health, the development of AI-based interventions addressing multi-morbidity over the lifecourse 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 takes into account the structures required to support multidisciplinary and multi-motivational 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 co-design and co-evaluation, 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, co-design, co-evaluation), 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 publicised appropriately and that community and individual benefits are realised – with evidence provided of proven potential.

4.4.2 Greater Assurances for Stakeholders

The design, testing, and generalisation of interventions from MELD requires 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 minimisation and mitigation of risk.

The approach of the SDF to *dynamic functional anonymisation, 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 pseudonymised, and therefore present a risk of re-identification when analysed 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 licence 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 re-identification risk assessment. The use of transparent, shared, non-repudiable audit records encourages compliant behaviours. Audit checkpoints for recording accesses datasets can be verified against their respective licence agreements. In some cases, multiple agreements are audited at the same point – for example, when the Data Analyst receives query results, the two licence 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 unauthorised 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 is 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 HRA and research sponsors.

The SDF model addresses the socio-technical 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 socio-technical 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., de-identification standards) and dataflows, and such efficiencies will allow for the potential for iterative ways of working and re-orchestration 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 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 data sets, 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 licence.

4.4.5 Facilitation of Localised 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 generalised and scaled nationally.

The SDF recognises that disruptive research and innovation often happens between trusted local partners working in placed based systems who address identified challenges together (NHS, n.d.). Projects are undertaken in the context of supportive national policies – where engagement in scale up

programmes turn 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, whilst 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 co-investigators also co-leads the SDF project, it is possible that data governance constructs may have influenced each project implicitly. However, we maintain that such overlap demonstrates in itself that the SDF is based on experience and not just 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 socio-technical 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 multi-stakeholder linked data (e.g., social determinants of health research) whilst 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 anonymisation 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, co-design, 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 data sharing and analysis projects using capabilities of functional anonymisation 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 multi-morbidity over the lifecourse – as an exemplar DSAP – in order to highlight the how the project can benefit from the SDF model when scaling the research to more complex datasets.

In this paper, we have presented our version of *datatrust services* within the specific context of the SDF. However, we recognise 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, stakeholder expectations). Whilst we must remain cognisant of the types of values embedded in

the design of *datatrust services*, and the extent to which these could act as constraints if re-deployed in other multi-party 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 flexible so that they can be generalised 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 licence, 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.

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
FAO = Functional Anonymisation Orchestrator
GDPR = General Data Protection Regulation
HRA = Health Research Authority
iCLIC = Interdisciplinary Centre for Law, Internet and Culture
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 Committees
NIHR = National Institute for Health Research (UK)
ONS = Office for National Statistics
PETs = Privacy Enhancing-Technologies
PI = Principal Investigator
RDA = Research Data Alliance
RM = Risk Management
SDF = Social Data Foundation
SD-WANS = Software-defined Wide Area Networks
TRE = Trusted Research Environment
UK = United Kingdom
UKHDRA = UK Health Data Research Alliance
WSI = Web Science Institute

List of Figures

Figure 1: SDF Governance Structure.....	10
Figure 2: A Datatrust Service Platform.....	14
Figure 3: Re-identification risk assessment for distributed query	17
Figure 4: MELD within the datatrust service platform.....	21

List of Tables

Table 1: Examples of Key Standardised Processes for all DSAPs	12
Table 2: Data Sharing and Analysis Project Template Types.....	16

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 & 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 (University of Southampton), Alistair Sackley (Web Science Institute, University of Southampton), Prof Mike Surridge (IT Innovation, 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 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.

Funding statement

The Social Data Foundation Project is partly funded and supported by the University of Southampton’s Web Science Institute (WSI) and Southampton Connect.

Competing interests

None.

Data availability statement

None.

Author contributions

Conceptualisation: MB; LC; BP; SSB; ST. Methodology: MB; SSB. Writing original draft: MB; LC; BP; SSB; ST. Writing – review & editing: MB; LC; WH; BP; SSB; ST.¹⁶ All authors approved the final submitted draft.

References

- Abrams, E.M. and Szeffler, S.J. (2020, July). 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](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/>; last 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>; last accessed 20 May 2021.
- Aitken, M., Tully, M. P., 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, K. H., Kaarakainen, M., Lugg-Widger, F., McGrail, K., McKenzie, A., Moran, R., Murtagh, M. J., Oswald, M., Paprica, A., Perrin, N., Richards, E. V., Rouse, J., Webb, J. and Willison, D. J. (2020). Consensus Statement on Public Involvement and Engagement with Data-Intensive Health Research. *International Journal of Population Data Science*. 4(1). <https://doi.org/10.23889/ijpds.v4i1.586>.
- 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; last accessed 21 May 2020.
- Banner, N. (2020, July 8). A new approach to decisions about data. *Understanding Patient Data*. Available at: <https://understandingpatientdata.org.uk/news/new-approach-decisions-about-data>; last accessed 20 May 2021.
- Bender, D. and Sartipi, K. (2013, June). HL7 FHIR: An Agile and RESTful approach to healthcare information exchange. In *Proceedings of the 26th IEEE International Symposium on Computer-based Medical Systems*, 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, November). 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/; last accessed 20 May 2021.
- Burström, B. and Tao, W. (2020, August). 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, P.R., Murtagh, M.J., Boyd, A., Williams, J.B., Dove, E.S., Wallace, S.E, Tassé, A-M., Little, J., Chisholm, R.L., Gaye, A., Hveem, K., Brookes, A.J, Goodwin, P., Fistein, J., Bobrow, M. and Knoppers B.M.

¹⁶ These author contributions are based on the CRediT Taxonomy – available at: <https://casrai.org/credit/>; last accessed 4 June 2021.

(2015, October). 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/>; last accessed 20 May 2021.

CARE Principles for Indigenous Data Governance. (2018, November 8). 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/>; last accessed 20 May 2021.

Carter, P., Laurie, G.T. 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>; last 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 & Data Office. (2020, September 16). Data Ethics Framework. UK Government Digital Services. Available at: <https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework-2020>; last accessed 20 May 2021.

Centre for Data Ethics and Innovation. (2020, July 20). 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>; last accessed 20 May 2021.

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

Data Linkage Western Australia. Available at: <https://www.datalinkage-wa.org.au/>; last accessed 19 March 2021.

Data Protection Act 2018 (UK). Available at: <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>; last accessed 24 May 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>; last accessed 21 May 2021.

Dodds, L., Szász, D. Keller, J.R., Snaith, B. and Duarte, S. (2020, April). 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/>; last accessed 20 May 2021.

Elliot, M., O'Hara, K., Raab, C., O'Keefe, C.M., 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, March 30). Introduction to Smart Contracts. Available at: <https://ethereum.org/en/developers/docs/smart-contracts/>; last 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>; last accessed 21 May 2021.

Ford, E., Boyd, A., Bowles, J.K.F., Havard, A., Aldridge, R.W., Curcin, V., Greiver, M., Harron, K., Katikireddi, V., Rodgers, S.E. 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, S.M. and Sturchio, J.L. (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>; last accessed 21 May 2021.
- Harrison, T. (2020, July 28). Putting the Trust in Trusted Research Environments. *Understanding Patient Data*. Available at: <https://understandingpatientdata.org.uk/news/putting-trust-trusted-research-environments>; last accessed 21 May 2021.
- Hawkes, N. (2013). Hospitals without walls. *BMJ*, 34, f5479. <https://doi.org/10.1136/bmj.f5479>.
- Hripcsak, G., Bloomrosen, M., FlatleyBrennan, P., Chute, C.G., Cimino, J., Detmer, D.E., Edmunds, M., Embi, P.J., Goldstein, M.M., Hammond, W.E., Keenan, G.M., Labkoff, S., Murphy, S., Safran, C., Speedie, S., Strasberg, H., Temple, F. and Wilcox, A.B. (2014, March). 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/amiainl-2013-002117>.
- ICES. Available at: <https://www.ices.on.ca/>; last 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>; last accessed 20 May 2021.
- Integrated Research Application System (IRAS). Available at: <https://www.myresearchproject.org.uk/>; last 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/>; last accessed 20 May 2021.
- ISO. (2018). ISO 27005 Information technology — Security techniques — Information security risk management. Available at: <https://www.iso.org/>; last accessed 20 May 2021.
- IT Innovation. (n.d.) MELD. University of Southampton. Available at: <http://www.it-innovation.soton.ac.uk/projects/ai-meld>; last accessed 4 June 2021.
- Jacobs, B. and Popma, J. (2019). Medical research, Big Data and the need for privacy by design. *Big Data & Society*. <https://doi.org/10.1177/2053951718824352>.
- Janssen, M., Brous, P., Estevez, E., Barbosa, L.S. 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, K. H., Ford, D. V., Jones, C., Dsilva, R., Thompson, S., Brooks, C. J., Heaven, M.L., Thayer, D.S., McNerney, C. and Lyons, R. A. (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>.
- Jones, K.H. and Ford, D.V. (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>.
- 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, R.R., Edmunds, R., Giarretta, D., De Giusti, M., L'Hours, H., Hugo, W., Jenkyns, R., Khodiyar, V., Martone, M.E., Mokrane, M., Navale, V., Petters, J., Sierman, B., Sokolova, D.V., Stockhouse, 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>; last accessed 21 May 2021.

- Mayer, R.C., Davis, J.H. and Schoorman, F.D. (1995). An integrative model of organizational trust. *The Academy of Management Review*, 20(3), 709-734. Available at: <https://www.jstor.org/stable/258792>; last 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>; last 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; last accessed 21 May 2021.
- Miller, F.A., Patton, S.J., 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., & Desai, K. (2020, December 14). Data Governance is Broken. *Information Week*. Available at: <https://informationweek.com/big-data/data-governance-is-broken-/a/d-id/1339635>; last accessed 21 May 2021.
- 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>; last accessed 20 May 2021.
- NHS Data Security and Protection Toolkit. Available at: <https://www.dsptoolkit.nhs.uk/>; last 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>; last accessed 20 May 2021.
- NHS Health Research Authority (HRA). (n.d.). What we do. Available at: <https://www.hra.nhs.uk/about-us/what-we-do/>; last accessed 21 May 2021.
- NHS. (2019, August). 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>; last 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/>; last accessed 21 May 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>; last accessed 21 May 2021.
- O'Hara, K. (2019, February). 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>; last accessed 20 May 2021.
- O'Hara, K. (2021, May). 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://dx.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. (n.d.) OWASP Top Ten. Available at: <https://owasp.org/www-project-top-ten/>; last accessed 20 May 2021.
- Pozen, D.E. (2005). The Mosaic Theory, National Security, and the Freedom of Information Act. *Yale Law Journal*, 115, 628-679, 2005. Available at SSRN: <https://ssrn.com/abstract=820326>; last 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; last accessed 21 May 2021.

- Public Health Research Data Forum. (2015, March). 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>; last 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, H. R., Albarqouni, S., Bakas, S., Galtier, M.N., Landman, B.A., Maier-Hein, K., Ourselin, S., Sheller, M., Summers, R.M., Trask, A., Xu, D., Baust, M. and Cardoso, M. J. (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 Databank. Available at: <https://saildatabank.com/>; last accessed 21 May 2021.
- Scott, K. (2018, April). 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; last 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*. <https://doi.org/10.1177/2053951719852969>.
- Smart Dubai and Nesta. (2020, March). Data Sharing Toolkit: Approaches, guidance and resources to unlock the value of data. Available at: <https://www.nesta.org.uk/toolkit/data-sharing-toolkit/>; last 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>; last accessed 20 May 2021.
- Spinney, L. (2021, January 2). 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>; last accessed 21 May 2021.
- Stalla-Bourdillon, S., Carmichael L. and Wintour, A. (2021). Fostering trustworthy data sharing: Establishing data foundations in practice. *Data & Policy*. <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>; last accessed 21 May 2021.
- Surridge, M., Correndo, G., Meacham, K., Papay, J., Phillips, S.C., 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)*. ACM, New York, NY, USA, 14-19. <https://doi.org/10.1145/3229616.3229621>.
- Surridge M., Meacham, K., Papay, J., Phillips, S.C., Pickering, J.B., Shafiee, A. and Wilkinson, T. (2019) Modelling Compliance Threats and Security Analysis of Cross Border Health Data Exchange. In: Attiogbé C., Ferrarotti F., Maabout S. (eds) *New Trends in Model and Data Engineering. MEDI 2019. Communications in Computer and Information Science*, vol 1085. Springer, Cham. 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://dx.doi.org/10.2139/ssrn.3716778>.
- The Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning systems. (2018). Amnesty International and AccessNow (eds.) Available at: https://www.torontodeclaration.org/wp-content/uploads/2019/12/Toronto_Declaration_English.pdf; last accessed 21 May 2021.

Triggle, N. (2021, February 25). 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>; last accessed 21 May 2021.

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

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

UK Department of Health & Social Care. (2021, January 19). 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>; last 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; last accessed 21 May 2021.

UK Health Data Research Alliance (UKHDRA): Innovation Gateway. Available at: <https://www.healthdatagateway.org/>; last accessed 21 May 2021.

UK Health Data Research Alliance. (UKHDRA). (2020, July). 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; last accessed 21 May 2021.

Understanding Patient Data and Ada Lovelace Institute. (2020, March). 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>; last accessed 21 May 2021.

University of Southampton. (2021). Social Impact Lab. Available at: <https://www.southampton.ac.uk/silab/index.page>; last accessed 20 May 2021.

Varshney, S. (2020, November 3). A Progressive Approach to Data Governance. Forbes. Available at: <https://www.forbes.com/sites/forbestechcouncil/2020/11/03/a-progressive-approach-to-data-governance/>; last accessed 20 May 2021.

Wessex Care Records. Available at: <https://www.wessexcarerecords.org.uk/>; last accessed 20 May 2021.

Winter, J.S. 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>; last 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)*. Association for Computing Machinery (ACM), New York, NY, USA, 191–200. <https://doi.org/10.1145/3287560.3287577>.