Information and Organization 33 (2023) 100451

Contents lists available at ScienceDirect

Information and Organization

journal homepage: www.elsevier.com/locate/infoandorg

Data governance spaces: The case of a national digital service for personal health data

Dragana Paparova [a,1,*], Margunn Aanestad [a,c], Polyxeni Vassilakopoulou [a], Marianne Klungland Bahus [b]

[a] Department of Information Systems, Faculty of Social Sciences, University of Agder, Norway
[b] Department of Law, School of Business and Law, University of Agder, Norway
[c] Department of Informatics, University of Oslo, Norway

ARTICLE INFO

Keywords:
Data governance spaces
Horizontal dynamics
Vertical dynamics
Data handling
Data handover

ABSTRACT

This paper investigates data governance empirically by conducting a retrospective study of the ten-year evolution of a national digital service for personal health data in Norway. We show how data governance unfolds over time as data become shared and itinerant across multiple actors. Building on our findings, we introduce the concept of data governance spaces to refer to the authorized relationships among multiple actors, which specify the boundaries of decision-making authority, rights, roles, and responsibilities around data processing. We contribute to the literature on data governance by distinguishing between a) authority multiplication, where data are handed over to other actors to serve diverse purposes triggering horizontal dynamics, and b) actor subordination, where authorities delegate data handling for uniform purposes triggering vertical dynamics. Overall, the paper extends prior research by showing how data governance unfolds beyond intra-, or inter-organizational boundaries and shifts attention to data's pivotal role, and the purposes for which data are collected, shared or used across multiple actors.

1. Introduction

Data governance has been receiving increasing attention among information systems (IS) scholars (Abraham, Schneider, & vom Brocke, 2019; Parmiggiani & Grisot, 2020; Winter & Davidson, 2020), and also across national and international political agendas (European Commission, 2020). The IS literature has commonly conceptualized data governance by building on information technology (IT) governance (Benfeldt, 2017; Fadler, Lefebvre, & Legner, 2021; Tallon, Ramirez, & Short, 2013), or modes of governance in inter-organizational settings (Jagals & Karger, 2021; Van den Broek & Van Veenstra, 2015). However, the data governance literature has not fully taken into account the role of data as they become shared and itinerant across multiple actors. We argue that data are not "just another" organizational asset. Due to their use-agnostic and semantic nature, data can decouple from the events they refer to (Alaimo, Kallinikos, & Aaltonen, 2020) and transform into larger objects (Aaltonen, Alaimo, & Kallinikos, 2021) as part of actors'

Abbreviations: IS, information systems; IT, information technology; GDPR, General Data Protection Regulation; EPR, electronic patient record; GP, general practitioner.

* Corresponding author.
E-mail addresses: dragana.paparova@uia.no (D. Paparova), margunn.aanestad@uia.no (M. Aanestad), polyxeni.vasilakopoulou@uia.no (P. Vassilakopoulou), marianne.k.bahus@uia.no (M.K. Bahus).
[1] Present/permanent address: Universitetsveien 25, 4630 Kristiansand, Norway.

https://doi.org/10.1016/j.infoandorg.2023.100451
Received 21 November 2021; Received in revised form 20 January 2023; Accepted 24 January 2023
Available online 6 March 2023

meaning-making processes. Data can also increase with use rather than being consumed, get diffused as they travel, and be shared without being depleted (Vassilakopoulou, Skorve, & Aanestad, 2019). This brings implications for data governance, particularly in the case of sensitive and personal data (Winter & Davidson, 2019), where the regulatory conditions differ from governing non-personal data. Therefore, data governance is not necessarily defined by managers within an organization, but frequently involves decisions by actors beyond organizational boundaries, including institutions regulating how such data are collected, shared and used.

We explore multi-actor data governance with personal health data as our empirical focus. Personal health data have been recognized as a key resource for innovation across healthcare services (Bardhan, Chen, & Karahanna, 2020). However, personal health data currently reside in siloed public or private actors' systems, and beyond isolated initiatives, routine sharing has not yet been achieved. Some of the core challenges in sharing personal health data lie in decisions related to data governance, including protecting intellectual property rights and privacy according to the legal provisions (Parmiggiani & Grisot, 2020), and retaining control once data are shared across multiple actors (Van den Broek & Van Veenstra, 2015). In 2018, the European Union introduced the General Data Protection Regulation (GDPR) aiming to bring more clarity to the governance of personal data (European Commission, 2016). However, the high abstraction level of GDPR, and its interpretation by regulators pose challenges to data governance, as organizations raise questions on how to enact the regulation (Greengard, 2018). Data governance across multiple actors concerning personal data remains a challenge impeding innovation, but has been only scarcely addressed in the IS literature.

This papers aims to advance research on data governance by using data, and not IT, as the focal point and account for the involvement of multiple actors. The research questions we seek to answer are *1) how to conceptualize data governance by accounting for the role of data,* and 2) *how does data governance unfold when data become itinerant across multiple actors?* To answer these research questions, we follow the data governance decision-making throughout the ten-year evolution of a citizen-facing digital health service for personal health data in Norway.

This paper offers conceptual and empirical contributions to the literature on data governance. First, this paper introduces the concept of *data governance spaces*, referring to the authorized relationships among multiple actors which specify the boundaries of decision-making authority, rights, roles, and responsibilities around data processing. Second, this paper shows how data governance can unfold across *vertical dynamics*, where actors *subordinate* to an authority, or *horizontal dynamics,* where authorities multiply and govern data separately. Third, this paper differentiates between *handling data* for uniform purposes and *handing data over* for different purposes, therefore pinpointing actors' purposes for collecting, sharing and using data. Fourth, this paper shows how data governance unfolds over time through an empirical study where multiple actors engage in decision-making around personal and sensitive health data.

The remainder of this paper is organized as follows. In the conceptual background, we problematize the existing IS literature which is commonly based on a framework-oriented understanding of data governance. We argue that data's distinctive nature requires further development of the data governance conceptualizations. In section three, we provide a description of the research design, methodology and case study. In section four, we present the findings and show how data governance dynamically unfolds as data become shared and itinerant across multiple actors. In section five, we induct concepts from the analysis of the empirical case. Finally, we discuss the added value of our concepts to the data governance literature and summarize the paper's key takeaways and limitations.

2. Conceptual background

2.1. The conceptual basis of IS literature on data governance

The growing body of IS literature focused on data governance commonly builds on the conceptual basis of IT governance, as Benfeldt (2017) noted. IT governance seeks to ensure that organizations utilize their IT assets to achieve strategic goals. With the increasing attention on data's potential business value, data are increasingly viewed as "assets" that also require similar governance in order to fulfill strategic purposes (Khatri & Brown, 2010; Otto, 2011). Data governance works often reference Weill and Ross' (2004) framework for allocating decision-making rights and accountabilities within several IT-related decision domains. While this framework is oriented towards governing traditional IT assets (hardware and software), Khatri and Brown (2010) proposed an alternative, but similar framework, covering a set of new decision domains relevant to data – data decisions, data quality, metadata, data access and data lifecycle – where the locus of accountability could be more or less centralized. Similarly, Tallon et al. (2013) argued for incorporating information governance as a novel decision area into the standard IT governance framework. This work draws on the governance mechanisms as defined in the IT governance literature, distinguishing between structural (relating to roles and responsibilities), processual (formal processes), and relational mechanisms (communication and coordination among stakeholders). These governance mechanisms are also central both in Abraham et al.'s (2019) conceptual framework, and in Fadler et al.'s (2021) mapping of data governance archetypes in organizations.

2.2. The work of establishing inter-organizational data governance

This reliance on the IT governance literature is problematic in the following ways. First, the IT governance literature is predominantly organization-focused, overseeing the empirical implications of data often flowing across organizational and sectorial boundaries (Janssen, Brous, Estevez, Barbosa, & Janowski, 2020). Governing data shared between organizations, in business ecosystems, or across public-private boundaries comes with distinct challenges from governing data within organizations. For instance, in their conceptual framework, Abraham et al. (2019) distinguish between the intra-organizational and inter-organizational scope of data governance. They discuss the need for companies to install distinct governance mechanisms in inter-organizational settings, such as

data integration and usage policies, data exchange standards, processes for interaction and collaboration, service level agreements, and data sharing agreements (ibid., p. 431). In practice, there is a large variety of inter-organizational relations and governance mechanisms, but little empirical research on how this variety maps to inter-organizational data governance (Jagals & Karger, 2021). Some of the few studies on inter-organizational data governance describe the archetypes of data collaborations (Van den Broek & Van Veenstra, 2015), stakeholders' coordination (Markus & Bui, 2012) and collective actions for decision-making (Benfeldt, Persson, & Madsen, 2020; Zhang, Sun, & Zhang, 2022). However, this remains an understudied area. A better understanding of governance in the context of inter-organizational data sharing is fundamental in collaborations encompassing public and private actors that seek to address grand challenges, where data not only generate organizational value, but are also a shared resource that can create societal value.

Several empirical studies describe the work involved in establishing data governance in organizations. Vilminko-Heikkinen, Brous, and Pekkola (2016) described the tensions and conflicts associated with implementing an organization-wide master data management initiative, as the top-down logic (inherent in any governance initiative) collided with various local logics. To investigate such challenges, Benfeldt et al. (2020) applied a collective action lens in their study of data governance in public sector organizations – where the diversity of responsibilities, a fragmented IT infrastructure, different professional domains, and multiple organizational objectives created challenges for successfully mobilizing the actors. The way these studies define their research problem – how various actors with heterogeneous (possibly contrary) interests and capabilities can govern common resources – has its parallel in studies on how shared information infrastructures emerge. For instance, Constantinides and Barrett (2015) investigated the dynamics among multiple actors during the development of a regional health information infrastructure. They propose a polycentric approach to govern infrastructure development, "where multiple governing units at differing scales can exercise considerable independence to make norms and rules within a specific domain" (ibid., p. 41), i.e., a nested and layered structure of governance rather than a monolithic one. Our study is informed by the literature on the evolution of information infrastructures, which investigates the involvement of multiple actors within and across organizations (Aanestad, Jolliffe, Mukherjee, & Sahay, 2014; Bowker, Baker, Millerand, & Ribes, 2009; Grisot, Hanseth, & Thorseng, 2014; Star & Ruhleder, 1994).

2.3. Data as a starting point for conceptualizing data governance

A second limitation in prior data governance research is the assumption that data can be considered an "asset" along with other assets, and therefore, governed likewise. In the classic IT governance framework by Weill and Ross (2004) the focus is on traditional IT assets and the data concern is diffused in the areas of IT architecture and IT infrastructure. Although the data governance literature argues that data differ from IT, data are usually considered "assets" and there is less attention to more fundamental questions about the nature of data. While there is recognition that data are context-contingent (Otto, 2011) and malleable (Abbasi, Sarker, & Chiang, 2016), these insights have not yet significantly impacted the conceptual groundings of the data governance literature. However,the nature of data has been more explicitly investigated by other literature streams within IS and such works provide valuable insights for conceptualizing data governance.

IS scholars have argued that data are conceptually different from IT, as they have a semantic (Alaimo et al., 2020) and use-agnostic nature (Alaimo et al., 2020; Constantiou & Kallinikos, 2015) and can be assigned various meanings as part of actors' value-creation. In these meaning-making processes, data transform from tokens into larger objects and commodities (Aaltonen et al., 2021), can be used in unforeseen ways (Lee, Zhu, & Jeffery, 2017; Susha, Janssen, & Verhulst, 2017), and for different purposes (Fadler & Legner, 2020). Data can also expand (increase with use rather than being consumed), diffuse (tend to travel), and be shared without being depleted (Vassilakopoulou et al., 2019). Data may also belong to various categories, where the use value, business criticality, and regulations may differ. For instance, some data may be openly shared (Bonina & Eaton, 2020), some may relate to proprietary knowledge regulated by intellectual property rights, and some may be personal data and thus subject to privacy regulations (Parmiggiani & Grisot, 2020). In the data governance literature, there has been limited attention on this variability of data aspects.

This paper argues that governing data is distinct from governing IT and this premise should serve as a basis for conceptualizing data governance. As Zhang et al. (2022) noted, beyond decision-making roles and responsibilities, data governance also needs to account for data stewardship (Rosenbaum, 2010), data ownership (Fadler & Legner, 2020; Van Alstyne, Brynjolfsson, & Madnick, 1995), and matters of data quality, privacy, and security (Abraham et al., 2019). These aspects are particularly significant concerning personal data, which have scarcely been at the focus of data governance studies in IS. For example, in their data governance framework, Abraham et al. (2019) distinguish between traditional data (master, reference, transactional) and big data (web, social media, biometric, machine-generated, streaming). However, no category is devoted to personal data.

Personal data are typically regulated by privacy-oriented legislation aiming to protect individuals. When personal data are aggregated and utilized for different purposes, such as by social media platforms, individual level regulations are insufficient (Viljoen, 2021). Winter and Davidson (2019) explored personal data governance by focusing on personal health data. The authors show how policymakers and regulators identified that the scale and scope of data exchanges and the appropriation of data-intensive technologies make existing laws and policies inadequate to fully protect patients' data. Here, regulations were not just triggers (DalleMule & Davenport, 2017; Khatri & Brown, 2010) or antecedents (Abraham et al., 2019) but actively shaped the data governance approaches. In another paper, Winter and Davidson (2020) highlight how person-generated healthcare data as highly unregulated data are governed by an interplay of organizational, technological and regulatory spheres.

Taken together, the more nuanced conceptualization of the nature of data, their mobility beyond organizational boundaries, the diversity of actors and interests, and the complexity of the regulatory landscape suggest that it is pertinent to rethink whether studying data governance around IT decision-making frameworks, or modes of governance, is sufficient.

3. Research approach

3.1. Case background

HealthNorway was launched in 2011 as a public healthcare digital service aiming to serve as citizens' single point of access to trustworthy, quality-assured health-related information. Subsequently, HealthNorway was extended with various interactive citizen-centric services, sharing data with hospitals' electronic patient records (EPR), General Practitioners' (GP) systems and municipal systems. Integrating with HealthNorway is very relevant for various public actors and private technology vendors. As of June 2022, 93% of citizens and residents use this service. HealthNorway is integrated with the EPR systems of 55% of GP offices, all Regional Health Trusts have made available at least one portal functionality to their citizens and the same holds for one out of every fourth municipality.

The citizen-centric functionalities provided at HealthNorway rely on the processing of personal health data; thus, they are subject to regulatory and legal frameworks HealthNorway and its collaborators must comply with. This legislation includes The Personal Data Act (regulating the processing of personal data, incorporating GDPR and special national rules for GDPR), Health Record Act (regulating the processing of health data when providing healthcare), Health Register Act (regulating the processing of health information for secondary use, such as health analysis, research, quality improvement, planning, management, and preparedness). These Acts also adopt the terms "data controller" and "data processor", as defined in the GDPR, where the data controller determines the purposes and means for processing personal data, while the data processor processes personal data on behalf of the controller.

As of 2016, HealthNorway is managed by a product board, including members from the health sector, such as the Health Directorate, Directorate of e-Health, The Public Health Institute, regional health authorities, municipalities, general practitioners, and citizens. This product board is part of the national governance structure for IT in healthcare, and the e-health board. The e-health board appoints the leader of the product board for HealthNorway and its mandate. The product strategy and roadmap for HealthNorway are developed and maintained as a collaboration between multiple public healthcare actors who define the scope of the digital service. The extension of the product with new functionalities is commonly organized as projects initiated by different public healthcare actors.

Providing citizen-centric functionalities at HealthNorway requires building trusted relationships between public and private actors for processing personal health data across authoritative sources. However, the National e-Health Strategy developed by the Directorate of e-Health (2021) raised that the unclear divison of roles and rules, unstable regulatory frameworks and legal uncertainties for data sharing challenge these public-private collaborations. The coordination across multiple healthcare actors on how to govern personal health data on top of the HealthNorway services is the main empirical focus of this paper.

3.2. Collection of empirical material

Our study is based on an interpretive paradigm (Alvesson & Sköldberg, 2010). We conducted qualitative research to map how data were governed across the actors involved as new functionalities were added. The extension of functionalities at HealthNorway is documented in publicly available information such as project and strategy documents, public presentations, online information resources, and data processing agreements. These were the primary information source for reconstructing the timeline of HealthNorway's growth and expansion. This empirical material was complemented with 13 semi-structured interviews with key persons who were (or had been) involved with HealthNorway's decision-making and one person who provided us with written responses. The informants included: product managers, product developers, portfolio managers, functional architects, enterprise architects, lawyers, technical consultants, and senior advisors. None of the informants were part of HealthNorway's team for the whole period of time covered in this paper.

The functionalities provided at HealthNorway required collaboration with various public and private actors, providing a multi-actor perspective on data governance. To acquire a more comprehensive understanding of the actors involved, we also conducted three interviews with private vendors working with person-generated healthcare data. All vendors included in the study had earlier attempts to integrate with HealthNorway, but during this study, such collaborations remained unrealized. However, these vendors are integrated with other parts of the public healthcare service delivery. Including informants directly and indirectly related to HealthNorway's evolution helped us gain a more comprehensive understanding of the challenges of sharing data across public and private healthcare actors. The informants from the private vendors' side include the founder, co-founder, and managing director. The collection of empirical material is summarized in Table 1

The interview guides used in semi-structured interviews were adapted to fit the informants' profile, background, knowledge, and position; they also reflected our knowledge of the case at that time. The interviews were executed in two batches. The first set of interviews started in June 2020 and lasted until April 2021. At this stage, we asked for participants' reflections on a broader set of topics, including the development of functionalities and data exchange arrangements. The second set of interviews was conducted from October 2021 to November 2022. In these interviews, we intended to grasp participants' reflections on recent developments towards personal data exchange, such as the Covid-19 pandemic, and get a more detailed understanding of the data governance decisions for the functionalities provided. During this phase, an interviewee read the empirical story and gave us their reflections on the narrative. The interviews were conducted online, with one exception (face-to-face), lasting approximately one hour and were fully transcribed.

Table 1
Summary of empirical material

Empirical material	Sources	Description
Semi-structured interviews (HealthNorway)	13	Duration: 1 h per interview, one interview of 1,5 h, and one interview of 2 h. Participants: product managers, product developers, portfolio managers, functional architects, enterprise architects, lawyers, technical consultants, senior advisors.
Semi-structured interviews (private vendors)	3	Duration: 1 h per interview. Participants: founder, co-founder, and managing director.
Written answers to interview questions	1	Confirm/correct information with a HealthNorway informant as an alternative to an interview.
Public documents	48	Product strategy documents, goal architectures, recommendations, guides for functionalities, evaluation of solutions, terms of usage and overview documents for data processing roles, private digital health apps, yearly reports of Norwegian Health Network and Directorate of e-Health.
Internal documents	5	Evaluation documents, report documents, market surveys, presentations.
Public videos	15	Length: 1–2 min. Short YouTube videos on citizen functionalities aimed at end users.
Video presentations	5	Length: 25, 30, 40 and 45 mins. Content on structured patient-generated data during Covid-19, digital forms, application programming interfaces management and ecosystem vision, aimed at stakeholders.
Presentation slides	8	Video consultation, patient-generated data, digital home follow-up services, application programming interfaces management, patient health records, municipal message exchange functionality.

3.3. Analysis of empirical material

The analysis of empirical material was iterated with its gathering, which helped direct our focus as we collected the empirical material. The analysis was performed in two phases. In the first phase, we conducted an inductive process analysis (Berends & Deken, 2021). We identified significant data governance events and ordered them sequentially. These events were reconstructed as a timeline of HealthNorway's evolution, focusing on extensions of eight functionalities, as presented in Fig. 1.

We realized that as the functionalities were extended, certain data governance decisions had to be repeated, but had different outcomes over time. Such decisions include the actors involved, the delegation of roles and responsibilities (data processors and data controllers), data storage, and citizens' rights over personal data stored about them. This phase uncovered the need to move beyond a framework understanding of data governance, and to account for data governance as changing over time.

In the second phase, we used the Gioia et al. (2013) method to induct concepts on top of our process analysis and weight our empirical material against the data governance literature (see Fig. 2). We ended up with 35 first-order informant terms related to the eight functionalities defined in our initial analysis. From there, we generated five second-order themes which showed how personal data were governed across multiple actors. We then used these insights to aggregate the second-order themes into more abstract concepts. In this phase, we realized how the same data could be governed differently by multiple actors depending on whether data are processed for the same or different purposes. Thus, we ended up with two aggregate dimensions: *data handling for uniform purposes* and *data handover for different purposes.*

With the insights from these two aggregated dimensions, we returned to the existing literature on data governance to inquire whether we discovered novel concepts (Corley & Gioia, 2011). We realized that the existing literature does not account for the role of data and actors' purposes for data processing. Additionally, the assumptions in extant literature were focused on top authorities, but not on multiple authorities governing the same data. Thus, we inducted the concepts of *vertical* and *horizontal dynamics* to show how actors can subordinate to an authority, or multiply their authorities when governing data. Finally, to provide a conceptual

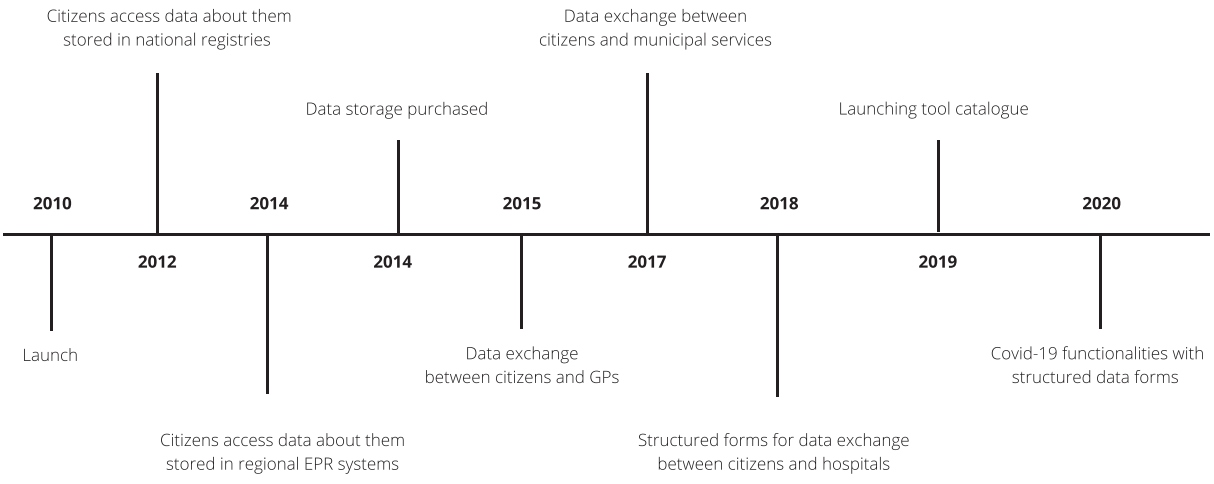

Fig. 1. Timeline of citizen-centric functionalities provided at HealthNorway

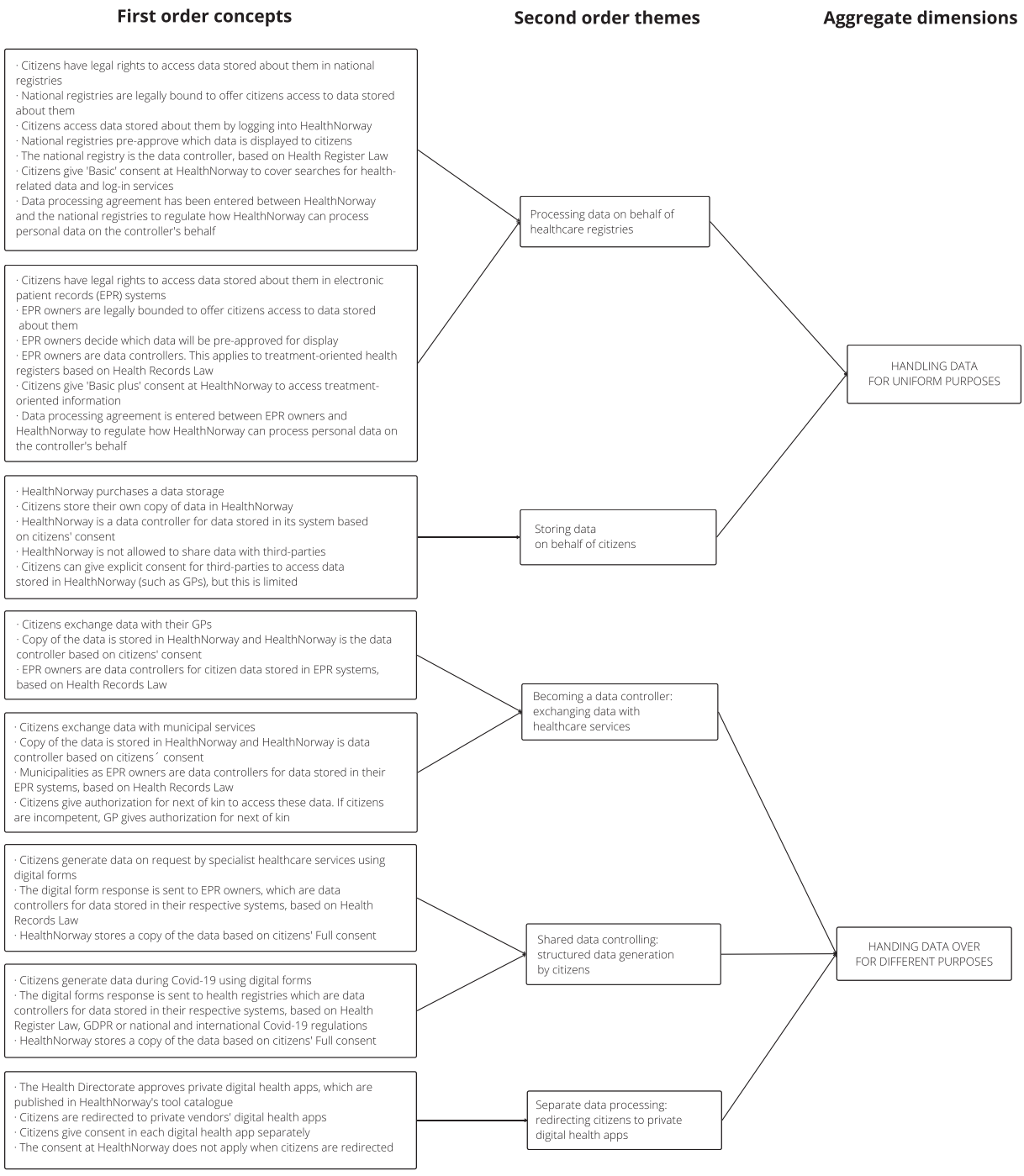

Fig. 2. Inducting concepts from the empirical material (Gioia, Corley, & Hamilton, 2013)

understanding of data governance by accounting for the role of data and the relationships between multiple actors, we generated the concept of *data governance spaces*. We elaborate on our findings and the concepts introduced in the sections that follow.

4. Findings: governing personal health data across multiple actors

This section presents how multiple actors engaged in decision-making around governing citizens' health data supported by HealthNorway's functionalities. Initially, HealthNorway provided quality-assured, general, and open information about illnesses and

treatments where no personal data were involved. Thus, we start our account with the first login services, i.e., the services involving personal health data.

4.1. Processing data on behalf of healthcare registries

The first personalized services HealthNorway offered were providing citizens with access to information stored about them in national health registries, such as vaccinations and drug prescriptions. For these services, HealthNorway had to collaborate with other health and care actors, such as the Public Health Institute (which owned the Vaccination Registry) and the Health Directorate (which owned the Prescription Registry). Initiating these services was triggered by citizens' legal right to access data stored about them and national registries' legal binding to provide such access. The healthcare registries decided to use HealthNorway as a channel for secure digital access. Technically, this was supported by HealthNorway introducing a login solution that identifies and authenticates the citizens before providing access to personal information stored about them. Citizens could only view, but not store a local copy of these data.

> *"Mainly we try not to store so much data because it is too complicated to process it, but HealthNorway has a lot of services where we do not store much data; we just provide access to it without seeing it. HealthNorway is saying, 'We know that you have some data at the Health Trust. We cannot open it, but we can help you see it,' so we cannot snatch the information on its way to the user. Many people think that HealthNorway knows a lot about you, but we do not. We are not allowed to read these data." (Informant, HealthNorway)*

In 2014, a second category of citizen-centric services was introduced, providing access to information stored in hospitals' electronic patient record (EPR) systems. This work was initiated by the Regional Health Trusts, and by citizens requesting access to personal data stored about them in the EPR systems. The Regional Health Trusts and citizens collaborated together with HealthNorway to map out the needs for providing these functionalities. The functionalities were available to citizens of the specific healthcare regions, but due to the systems' different maturity levels, the information citizens could access differed from region to region.

The processing of personal data in national registries was regulated by the Health Register Act; the same applies to the regional EPR systems which were regulated by the Health Record Act. In this case, the law determined and directly appointed the data controllers as it imposed a duty on the registries to collect and process personal data related to the tasks they fulfill. The law also obliged the registries to provide citizens with access to personal data stored about them. The registries could decide which information should be pre-approved for display to citizens in HealthNorway within their defined purposes and had to enter into a data processing agreement, which regulates how HealthNorway can process personal data on their behalf. However, HealthNorway also had to establish its own legal basis for processing personal data related to authentication and authorization when citizens log in. It was decided to introduce the option for citizens' consent, grouped in three categories: Basic, Basic Plus or Full consent. An informant shared some of the discussions related to defining the consent structures:

> *"When we created the structures of the consents, we were in dialogue with the data authorities and they said that you should be able to choose not to do everything. So, the reason for us having a layered structure of consent, is because it is kind of decent to allow citizens to use parts of the functionality, but not all, and then try to find out what is possible to sort of exclude in these different layers. Then, medical records were considered something that was more sensitive to citizens than some other information. Therefore, we wanted to make a structure whereby one could say, 'Okay, I want to use these other things, but I do not want to use that.'" (Informant, HealthNorway)*

The different consent categories allowed citizens to choose whether or not they wanted their personal health data to be processed, control which information could be processed and what it could be used for. For example, providing citizens with access to data stored about them in national registries required consent to the category Basic, which covered the processing of multi-purpose health-related personal information. However, the regional EPR systems stored treatment-related personal information, and this required consent to the Basic Plus category.

Therefore, for these initial functionalities the data governance authority was placed with the healthcare registries. The healthcare registries determined the purposes for processing citizen data, specified how citizens could exercise their rights to access personal data stored about them, as well as delegated roles and responsibilities to HealthNorway on how to handle data within the specified purposes.

4.2. Storing data on behalf of citizens

In 2014–2015, HealthNorway started working on offerring interactive services where citizens could send and receive messages with healthcare services, instead of solely accessing data stored elsewhere. This service required that HealthNorway provides a storage where citizens could keep their own copy of the messages, which would be secure, even if the healthcare services changed their EPR system providers. The storage used up to then was evaluated as being not comprehensive enough for storing this type of personal health information, so HealthNorway purchased a new data storage solution. The core principle was that the data stored in HealthNorway belongs to the citizen, not to the healthcare services. The legal basis for storing these data was citizens' consent, and HealthNorway took the role of a controller for the data stored in its system. The consent provided a legal basis for HealthNorway to store citizens' personal data, but not to share it with third parties, unless such sharing is preapproved by the citizens.

> *"The objective has been to provide the opportunity that you can, as part of what we provide, collect data that you want to share with someone, but this does not mean that HealthNorway is allowed to share it with others without your consent. So, it is always the*

inhabitants sharing data with someone; it is never the portal sharing data with someone without the inhabitants asking us to." (Informant, HealthNorway).

Acquiring a storage as a technical capability, and citizens' consent as a legal basis, did not imply that HealthNorway could save a copy of just any personal data stored about citizens in external systems. Instead, whether storing a copy was allowed or not, also had to be specified within the agreements between HealthNorway and the healthcare actors it collaborated with. For example, HealthNorway could not store a copy of the data accessed from the Prescription Registry, as the data processing agreement specified that HealthNorway acts on behalf of the registry and within its defined purposes. An informant explained how storing data at HealthNorway is aimed at citizens as end users, which differs from the purposes for storing citizens' data in other public healthcare systems whose end users are healthcare personnel.

"HealthNorway is important because there is some information that you should be able to collect and you should be able to share, but I think it is more important to use HealthNorway for information that you are collecting for yourself, rather than for sharing information that resides in a third party system, for instance at your healthcare provider. […] So, it is kind of sharing of responsibilities and making sure that the portal is something that is a tool for you as a citizen, and other systems should be tools for instance for healthcare personnel who need the data." (Informant, HealthNorway)

Therefore, the governance of data stored in HealthNorway was specified within the legal provisions of consent, and HealthNorway processed data on the citizens' behalf. The intention was that citizens would also use this storage to add or generate their own data (such as from wearables and welfare technologies) and decide whether they want to share these data with others (such as for research purposes). However, as of 2022, the primary usage of the storage was collecting copies of citizens' personal health data, due to lack of prioritization of its expanded usage. Regardless, the storage provided a significant basis for the functionalities further provided.

4.3. Becoming a data controller: exchanging data with healthcare services

As of 2014, many GP offices started offering interactive services for citizens. However, GP offices collaborated with different EPR vendors, but the functionalities and interfaces provided, and the security levels across the solutions differed significantly. HealthNorway started collaborating with the healthcare actors on providing common functionalities for message exchange, booking or changing appointments, and requesting or renewing prescriptions, which can bridge the differences across the back-end systems. Providing these services also required collaboration with the private EPR system vendors who had to implement the technical integrations, and the rollout was in 2015.

The processing of personal data for these functionalities had to be kept legally separate from other data processing arrangements at HealthNorway. For example, citizens could access prescriptions stored about them in the Prescription Registry, and renew prescriptions if their GP approved this through the HealthNorway functionalities. However, due to the different legal basis for processing data with national registries and GPs, these two functionalities had to be put on a separate page.

"In HealthNorway you can get a list of your medications, and you can see prescriptions and you can renew prescriptions. However, seeing the prescriptions is based on the regulation that handles the prescriptions, and requesting new prescriptions is based on the data processing agreement with the general practitioner and you are not allowed to mix those two. They [HealthNorway] wanted to put a button on your prescription lists where it says 'renew prescription', but they were not allowed to. They had to have those functions on separate pages because of the way the whole legal framework is built. The legal framework sort of prevents usability." (Informant, HealthNorway)

In 2017, information exchange was also made available for citizens who received municipal health and care services (e.g. nursing services offered in elderly patients' homes). Besides the citizens, their authorized contacts (next of kin) could now also interact with the municipal health services. This required a new agreement, which can include next of kin in the digital interaction. If the citizens were competent to give an informed consent, they could enable these services themselves. If they were not competent, the next of kin could complete a form that is confirmed by the GP and be granted access at HealthNorway.

In the previous services for accessing information, HealthNorway solely acted as a data processor for data controlled by the national registries. Regarding services involving information exchange, EPR owners were data controllers only for the citizen data stored in their respective systems, and they were appointed this role based on the Health Record Act. However, a copy of the data was now also handed over to HealthNorway, and HealthNorway was the data controller for it, based on citizens' Full consent. The reason for EPR owners not being data controllers for the copy stored in HealthNorway was due to them not having formal control over the data processing taking place in external systems. An informant exemplified how data stored in HealthNorway are governed independently from data stored in other healthcare actors' systems, as in this case HealthNorway does not act on their behalf:

"Once the data is stored in HealthNorway then the data belongs not to the health provider but to the inhabitant or to us on behalf of the inhabitant, because the inhabitant should be able to delete it. The health provider cannot ask us to keep that data because they are going to use it later for reviewing their own work or something; it is the inhabitant that will be in charge of that data." (Informant, HealthNorway)

Therefore, storing the same data in different systems was subject to two authorities that could separately determine the purposes and means under which they process personal information. HealthNorway stored a copy on behalf of the citizen the data was about, where the purposes and means for data processing were regulated through citizens' consent. The purposes and means of GP and

municipal systems were regulated by law, obliging them to store treatment-related information and always keep it updated. Therefore, the same data were subject to different authorities, specifying distinct rules for data governance.

The authorities could also delegate roles and responsibilities, but only for the data processed for their specified purposes. For example, some GP offices and municipalities purchased video consultation services provided by private vendors. When citizens used such video consultations services at HealthNorway, some personal information could be disclosed to the private video providers. In that case, the GPs or municipalities enter a data processing agreement with the private vendor systems they use; HealthNorway just redirects the citizen to that particular service. Therefore, the private providers of video consultations process data on behalf of the healthcare services, but not on behalf of HealthNorway.

4.4. Shared data controlling: structured data generation by citizens

Ever since the launch of the first interactive services in 2015, HealthNorway was collaborating with the regional health authorities to map out the needs for information exchange between specialist healthcare services and citizens. Instead of exchanging messages, specialist healthcare services raised the need for collecting structured data. The structured data forms available on the market then did not support sending or receiving data where the sender and the recipient used different systems. The healthcare actors decided that HealthNorway will provide an architecture of common components to support structured data exchange between different systems. This included standardized interfaces to integrate with private vendor forms that public healthcare actors already use, as well as a catalogue of digital forms which can be reused across healthcare services. The services were rolled out in 2018–2019, enabling a controlled way for hospitals to collect e.g. pre-consultation information, patient-reported outcome measures (PROMs) and patient-reported experience measures (PREMs).

During the Covid-19 pandemic multiple citizen-centric services were released using digital forms, such as symptoms reporting, symptoms checking, and customized reports. Some forms provided at HealthNorway were also collected by the National Institute of Public Health for better planning during the pandemic, such as deciding which citizens to prioritize for testing in the municipalities or which results to analyze first in the labs. Therefore, digital forms were used to exchange structured data with various healthcare actors who had different purposes for processing personal data.

Similarly to the previous services, HealthNorway took the role of data controller for the copy of the form stored in its components based on citizens' Full consent. The data controller responsibility for the health registries or EPR system owners as receivers of the digital forms was delegated to them by the Health Register Act or the Health Record Act, respectively. However, decisions also had to be made on how to govern data in the common components developed by HealthNorway and before these data were transferred to the health registries or EPR systems. It was assessed that there should be only one data controller for these components, which would clarify the roles and responsibilities. Since HealthNorway developed the common components, it also took the role of data controller for data processed in these components, but this role only applied until citizens' data are handed over to the health registries or EPR owners.

> *"If one solution is [only sending a personal] link for filling in a form, then they [the health registries] only use HealthNorway as a mailbox. However, if they send you something like 'This is a form,' rather than 'This is just a message,' they could also in the metadata say something about it, 'There should be a reminder if you have not done this task in a while' […] So, with the registries in [Region Middle] when they send you a form you are redirected to the form filler of the register, e.g. the health register for brain disease or something. You are in that form filler but because they cannot store your data before you say 'I want to store these data in the register', the buffer storage is done at HealthNorway. Then, when you press the final button saying, 'I want to actually store, send this to the register,' then it is stored directly in the register as well, but you then will have a copy of your data at HealthNorway." (Informant, HeatlhNorway)*

Similarly to the previous services, when using digital forms provided by private vendors, citizens would be redirected instead of filling this form at HealthNorway. The private digital form vendors processed citizens' data on behalf of the national, regional or municipal public healthcare actors who determined the purposes for such processing, but not on behalf of HealthNorway.

Therefore, the digital form services involved multiple healthcare actors who exercised authority over their own data processing and could independently determine the purposes and means or delegate roles and responsibilities for the data processed on their behalf. This did not imply that two or more actors were responsible for the same data processing. Instead, there was a clear division of responsibilities on where one actor hands data over to another.

4.5. Separate data processing: redirecting citizens to private digital health apps

During 2018, multiple private digital health apps were available for citizens, but there were no national criteria to evaluate which apps were safe to use as part of the official healthcare service offerring. The public healthcare authorities started discussing how to provide a place where citizens could find quality-assured digital health apps. They decided that such apps will be published on the HealthNorway website, and the service called "tool catalogue" was launched in 2019. Inclusion in the tool catalogue was determined by the Health Directorate, which assessed case by case whether the digital health apps fulfilled the criteria around information security, the health benefits of the apps' content, and the public need for including such apps as part of the official healthcare service offering.

> *"There are agreements with the health provider that is responsible for the app, so we have an agreement with the Health Directorate that is responsible for several of the applications. We have an agreement that on behalf of the Health Directorate this application is made available to the population in the catalogue. Most of them do not require you to log in, therefore redirection is sufficient to provide to the need." (Informant, HealthNorway).*

It was decided that the Health Directorate would take the responsibility for the digital health apps, while HealthNorway would only enter into agreements with the Health Directorate, but not directly with the private vendors providing these apps. One reason for such partitioning of responsibilities was due to the large size and variance of the private vendor market, whereas HealthNorway as a product was not intended to cover the overall sector needs but provide an entry-point for citizens into their personal health information. However, another significant concern was the limited scope of control that HealthNorway has over data processed in the private vendor systems, particularly when the purpose of such processing is defined by citizens' consent on both sides. The possibility of HealthNorway taking the data controller responsibility for processing data in the digital health apps was considered too risky. An informant shared some of the possibilities discussed:

> *"We had a meeting where we discussed the possibility of us taking the controller responsibility for the information in the different tools that we let people out to at HealthNorway; that is one alternative. However, the consequence of that is that we have to have the control of what happens in the tools. So, the question is how realistic is that and how are we going to follow up on all these agreements that have to be put in place because we are talking about a large scale. That is one possibility; the other possibility is to have a more strict routine for maybe a self-declaration from the tool – that is something we have discussed – to ensure that they are compliant with the GDPR and that they have sufficient information security and those things. So, the self-declaration form regarding the privacy and information security together with the responsibility that lies at the Health Directorate when it comes to the clinical purpose of the tool." (Informant, HealthNorway)*

The healthcare actors also discussed the potential benefits of acquiring a dedicated Act that would give HealthNorway the same legal status as the health registries whose purposes for data processing are regulated by law. The attempts to acquire a dedicated HealthNorway Act were not triggered by the need to control data processing in the digital health apps, but could strengthen the basis for HealthNorway taking on the data controller role for these services. However, as of 2022, such regulation is still not in place. An informant shared how the current consent option limits the possibilities for data processing, unlike a dedicated law:

> *"The lack of HealthNorway law has given us quite a few restrictions because we have to keep the consent from the citizen valid at all times, and with the development process we have, things are developing really quickly. It is a really hard job to make sure that we are still within the scope of the consent that citizens have given." (Informant, HealthNorway)*

Unlike the previous functionalities where the data were processed in collaboration with healthcare actors whose purposes were regulated by law, now the purposes for processing data in each digital health app were regulated by citizens' consent. Neither HealthNorway nor the digital health app vendors had the formal authority to control how data are processed once they are handed over to an external system. Also, if HealthNorway and the digital health apps processed the same data, the compatibility of purposes would have to be evaluated case by case. Thus, it was decided that technically, the apps in the tool catalogue would be stand-alone; citizens would be redirected and give consent in the respective app. Both HealthNorway and the digital health app vendors would be the controllers for the data processed in their own systems. However, neither could delegate roles and responsibilities to the other, or impose restrictions on the purposes the data could be processed for.

5. Analysis: re-conceptualizing data governance

5.1. Purposes for data processing: data handling and data handover

Our empirical findings show how data were processed for various purposes by multiple actors, which required renegotiating data governance instead of delegating responsibilities by one actor or from the top. To answer our first research question: "How to conceptualize data governance by accounting for the role of data", we show how multiple actors can process data for uniform or different purposes by distinguishing between data handling and data handover.

Data are handled when multiple actors process data on behalf of another actor who specifies uniform purposes for data processing. In our case, data are handled when HealthNorway accesses citizens' personal data on behalf of the healthcare registries as data controllers but such processing was only within the purposes defined by the registries. *Data are handed over* when multiple actors copy data, and each actor can determine different purposes for its own data processing. Our findings show how in the case of message exchange, the public healthcare actors were data controllers for their data processing based on law, and HealthNorway was the data controller for the copy of the same data stored in its system based on consent. Therefore, each actor independently determined the purposes for processing the same data.

Defining whether data are being handled or handed over has implications for conceptualizing data governance, as it shows how data processing is defined around specific purposes which can be uniform or different across multiple actors.

5.2. Vertical and horizontal data governance dynamics

To answer our second research question, "How does data governance unfold when data become itinerant across multiple actors?"

Table 2
Horizontal and vertical data governance dynamics

Data governance dynamics	Actors	Data processing	Empirical example
Vertical data governance dynamics	**Authority delegates** roles and responsibilities within the specified purpose **Actors subordinate** and act on behalf of the authority	**Handling data** for a uniform purpose	Processing data on behalf of healthcare registries Storing data on behalf of citizens
Horizontal data governance dynamics	**Authority multiplies** and each authority specifies its own purpose for data processing **Each authority delegates** roles and responsibilities within its specified purpose	**Handing data over** for different purposes	Becoming a data controller: exchanging data with healthcare services Shared data controlling: structured data generation by citizens Separate data processing: Redirecting citizens to private digital health apps

we distinguish between vertical and horizontal data governance dynamics.

Vertical data governance dynamics refer to the *subordination* of rights, roles, and responsibilities under the authority of a specific actor. In this case, *data are handled* by multiple actors on behalf of another actor who holds the authority for the data processing. The authority defines the purposes for "why" data are being processed, and other actors can act solely within these specified purposes. The "how" or the technical and organizational means on how to achieve those purposes can be delegated to other actors. However, even if responsibilities are delegated, the authority is responsible for the data processed on its behalf. Other actors can process the data only for the concrete responsibilities delegated by the authority and cannot determine their own purposes for processing the same data. For example, the Prescription or Vaccination Registries delegated the responsibility for providing access to personal data stored about citizens to HealthNorway. HealthNorway could only process data on their behalf, not for its own purposes.

Horizontal data governance dynamics refer to the *multiplication* of authority, rights, roles, and responsibilities across multiple actors. In this case, data are *handed over* from one actor to another, and each actor separately fulfills the obligations of being an authority. Therefore, multiple authorities separately determine the purposes "why" and the means "how" to achieve such purposes for processing the same data. This does not indicate that the responsibility for being an authority is delegated from one actor to another, where one actor fulfills some obligations for being an authority while the other fulfills the rest. Instead, each actor independently fulfills the responsibilities for being an authority, defines its own purposes for processing data, delegates roles and responsibilities within the specified purposes and is responsible for the data processed on its behalf. In our case, both HealthNorway and the EPR owners were data controllers for the message exchange or digital form functionalities. HealthNorway was the authority for the data copied in its own system, and the EPR owners were the authorities for the data stored in their respective systems, and responsible for the private vendor systems processing data on their behalf.

The horizontal and vertical data governance dynamics show how actors either subordinate or multiply their authorities, rights, roles, and responsibilities when governing data (see Table 2). However, such subordination or multiplication is not static, where one actor is either an authority, or solely acting on behalf of others. Instead, as new actors, data or purposes are added, actors can take on various roles for different data processing, making data governance dynamic and changing over time.

5.3. Data governance spaces

To provide a comprehensive understanding of multi-actor data governance and foreground the role of data, we introduce the concept of data governance spaces. We define *data governance spaces* as the authorized relationships among multiple actors which specify the boundaries of decision-making authority, rights, roles, and responsibilities around data processing. The definition of data governance spaces consists of three pivotal parts: multiple actors, authorized relationships, and actors' boundaries. First, data governance spaces are *multi-actor*, and not single-actor; however one actor can simultaneously participate in multiple data governance spaces by taking on different roles. The same actor may act as a controller for certain data processing and as a processor for another. Second, data governance spaces specify *authorized relationships* among actors. These relationships, whether unfolding across horizontal or vertical dynamics, either subordinate or multiply actors' authorities, rights, roles, or responsibilities. Therefore, unapproved disclosure of data to a third party, such as in data breaches, does not define a data governance space. Third, in data governance spaces, actors can exercise their authority, rights, roles and responsibilities within specific *boundaries*. These boundaries are defined by the transfer of data responsibilities, where data are handled for a uniform purpose or handed over for different purposes. Therefore, the boundaries are not determined by organizations, or the IT systems processing data, but determined by actors' purposes for processing data.

Our findings show how HealthNorway was simultaneously participating in multiple data governance spaces with public healthcare actors, such as national, regional and municipal services. However, data governance spaces were not enacted between HealthNorway and the private vendors, due to the inability to establish authorized relationships, and the differences in purposes for processing personal data. The data governance spaces and their horizontal and vertical dynamics are illustrated in Fig. 3.

6. Discussion

This paper contributes to the literature on data governance in the following ways. First, we contribute with an improved

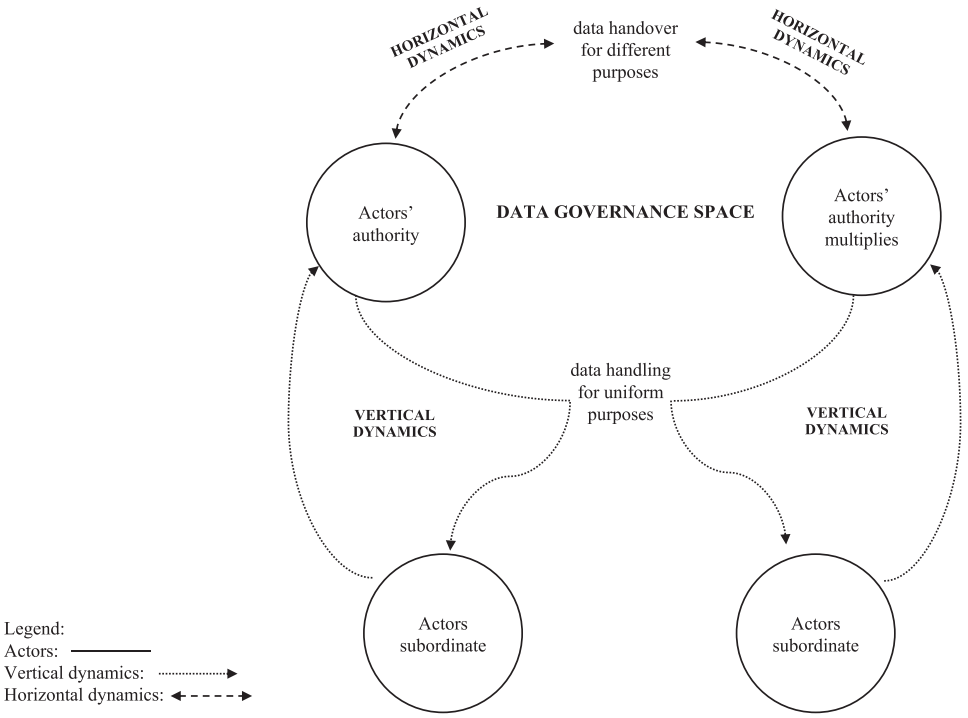

Fig. 3. Illustration of data governance spaces and their horizontal and vertical dynamics

understanding of "what" is being governed by showing how governing data differs from governing IT. IS research on data has shown how throughout their lifecycle, data decouple from the digital technologies that produce or carry them (Alaimo et al., 2020) and get aggregated and repurposed into larger objects and commodities (Aaltonen et al., 2021). This paper argues for setting data at the core of conceptualizing data governance. By distinguishing between data handling and data handover, we show how data can be processed for uniform or different purposes by various actors. We argue that the purposes for data processing, and not the IT systems data are processed in, should be the guiding principle when conceptualizing data governance. This builds on IS works discussing how data differ from IT, as they can generate value through processes of signification, meaning-making and knowledge production, instead of by creating composite entities in the form of IT artefacts (Alaimo et al., 2020).

Moreover, the data governance literature commonly refers to data as assets (Benfeldt et al., 2020; Fadler et al., 2021; Janssen et al., 2020; Nokkala, Salmela, & Toivonen, 2019; Van den Broek & Van Veenstra, 2015) implying that like other assets, data can be owned by organizations. By distinguishing between data handling and data handover, we show how data can be replicated across multiple actors, which separately determine the purposes for data use and define their own data governance rules. Furthermore, our findings show how in the case of personal data, data governance is also shaped by the rights of the data subjects they are about. This contributes to existing debates on the lack of clarity in determining data ownership (Fadler & Legner, 2020; Van Alstyne et al., 1995), as we show how data cannot be owned by organizations similarly to other types of assets governed.

Second, we contribute to the understanding of "who" governs data. Within organizations, the data governance literature commonly assigns this responsibility to the data governance leaders, councils, or offices (Abraham et al., 2019), data stewards (Rosenbaum, 2010), or data owners (Fadler & Legner, 2020). The literature on inter-organizational data governance shows how governing data requires coordination by actors around overarching goals (Jagals & Karger, 2021; Susha et al., 2017), but still assumes the presence of *top* authority for data governance, particularly regarding personal data. For example, Van den Broek and Van Veenstra (2015) have argued that in the context of personal health data, governance should be hierarchical due to legal implications. Our findings show how personal data can be governed by multiple authorities, which can delegate roles and responsibilities to other actors processing data on their behalf. By distinguishing between vertical and horizontal dynamics we show how actors can either subordinate to an authority, or govern data independently by becoming the authority themselves. The concepts help us understand how roles and responsibilities around data are not simply delegated, access is not exclusive, and authority can shift from one actor to another.

Third, we contribute to the understanding of "how" data are governed. Our findings show that decisions about governing data are not simply managerial, but can be delegated from outside organizational boundaries. Extant literature on data governance acknowledges the importance of legal frameworks and regulations, particularly in the context of personal data (Van den Broek & Van Veenstra, 2015; Winter & Davidson, 2020). However, we show how the law is not simply an antecedent (Abraham et al., 2019) or an environmental factor (Fadler et al., 2021) but another actor that actively shapes data governance, including delegates roles and responsibilities and determines the purposes for data processing. By introducing the concept of data governance spaces we show how

data governance is not determined by intra- and inter-organizational boundaries but by the actors involved, their authorized relationships, and their purposes for data processing. Therefore, we move beyond conceptualizing data governance as a framework (Abraham et al., 2019) or a mode of governance (Jagals & Karger, 2021; Van den Broek & Van Veenstra, 2015), to encompass how data governance changes over time across horizontal and vertical dynamics, as new actors, authorized relationships or purposes for data processing are introduced.

This paper also has implications for practice, as it shows how data governance does not always fit pre-existing frameworks due to data's semantic and use-agnostic nature. Instead, actors must assess whom they process data with, and how and why are data processed to determine who should take the data controller or processor role in the specific circumstances. This does not indicate that data are governed without any structure but that the frameworks can direct; however they cannot always predetermine the relationships occurring in multi-actor settings.

7. Concluding remarks and limitations

Personal health data – the empirical focus of this paper – are recognized as a key resource for innovation across healthcare services. Understanding data governance in such multi-actor contexts is crucial for enabling innovation in the healthcare domain and across other sectors seeking to address grand challenges requiring data-centred collaborations.

This paper contributes to the literature on data governance by introducing the concept of data governance spaces and their horizontal and vertical dynamics of change over time. The concepts are inducted from an empirical study on the evolution of data governance for digital health services in Norway, which brings certain limitations. First, it raises questions on whether the knowledge gained from a single-case study on governing sensitive and personal data in a highly-regulated environment can be applicable beyond this context. Although we conceptualize data governance through a study following the governance of personal health data in the European legal context, we believe the concepts introduced in this paper are generalizable across contexts. For instance, processing non-personal data might not be subject to data protection and privacy laws but to other types of actor agreements, such as intellectual property rights or contractual agreements. In commercial platforms for non-personal data, the platform owner may possess the intellectual property rights for data processed by third parties on its behalf, thus implying vertical data governance dynamics. However, if intellectual property rights are distributed, for instance, in an arrangement where each actor owns the data produced in its own components and separately defines the rules for governing such data when collaborating with other actors, the data governance dynamics would be horizontal.

Second, as raised in the methodology, the study's ten-year narrative was reconstructed through empirical material collected over approximately two and a half years. Therefore, the empirical story was constructed retrospectively and reflected the memory, interpretations, and opinions of informants while gathering the empirical material. We aimed to overcome such limitations by relying on official documentation encompassing the ten-year period covered in the study; however, this documentation does not fully account for the discussions and decisions occurring in real time. Moreover, collecting the empirical material was concentrated around a focal organization and a selection of private vendors, whereas the perspectives of other public or private collaborators were constructed through indirect inference. Therefore, this is another limitation of our study.

Future research can study data governance across different multi-actor settings, including perform comparative studies within and outside the highly-regulated European environment. Furthermore, in our case, data governance spaces were not enacted between the public organization studied and the private actors. Examining data governance in public-private collaborations, particularly in the context of personal data, requires exploration and could uncover novel data governance insights. The concepts this paper introduced can be developed further, and future research could show how data governance spaces unfold across different multi-actor settings.

CRediT authorship contribution statement

Dragana Paparova: Investigation, Conceptualization, Methodology, Formal analysis, Visualization, Writing - original draft, Writing - review & editing. **Margunn Aanestad:** Supervision, Conceptualization, Formal analysis, Writing - review & editing. **Polyxeni Vassilakopolou:** Conceptualization, Visualization, Writing - review & editing. **Marianne Klungland Bahus:** Validation.

End notes

1. Personal Data Act: Personopplysningsloven: 2018- 06-15 no. 38
2. Health Register Act: Helseregisterloven: 2014-06-20 no. 43
3. Health Record Act: Pasientjournalloven: 2014-06-20 no. 44

Data availability

The authors do not have permission to share data.

Appendix

Table A1
Summary of citizen-centric functionalities added over time.

Functionality	Year	Description	Citizens' rights	Actor roles	Legal basis
Accessing information in national health registries on behalf of citizens	2012	Citizens log into HealthNorway but are redirected to Prescription or Vaccination Registry to see personal information about vaccination and prescriptions	View access	Data controller: National Health Registries; Data processor: HealthNorway	Health Register Act, Personal Data Act, Basic consent
Accessing information in regional health registries on behalf of citizens	2014	Citizens log into HealthNorway but are redirected to see personal information from regional EPR systems	View access	Data controller: Regional Health Registries; Data processor: HealthNorway	Health Record Act, Personal Data Act, Basic consent
Storing data on behalf of citizens	2014	Citizens can save their own copy of data stored someplace else or generate their own data	View, write, edit, save, delete	Data controller: HealthNorway	Citizens' consent
Information exchange between citizens and GP offices	2015	Citizens can book and change an appointment, request, or renew prescriptions and exchange messages	View, write, edit, save, delete (for data stored in HealthNorway)	Data controllers: GP owners for original data and HealthNorway for copy; Data processors (if any): Private vendors, on behalf of GP owners	Health Record Act Full consent required for message exchange, other services covered with Basic or Basic Plus
Information exchange between citizens and municipal services	2017	Citizens or next of kin can book and change an appointment, exchange messages and get notifications	View, write, edit, save, delete (for data stored in HealthNorway)	Data controllers: Municipal services for original data and HealthNorway for copy	Health Record Act Full consent required for message exchange, other services covered with Basic or Basic Plus
Structured data forms for data exchange between citizens and hospitals	2018	Citizens can exchange digital forms with specialist healthcare services. The form can either be filled in at HealthNorway or citizens are redirected to a private vendor form via link	View, write, edit, save, delete (for data stored in HealthNorway)	Data controllers: Regional Health Trusts and HealthNorway for copy; Data processors (if any): Private vendors, on behalf of healthcare services	Health Register Act or Health Record Act Full consent to save a copy
Structured data forms for data exchange between citizens and national services during Covid-19	2020	Multiple citizen-centric services provided using structured data forms, such as: symptoms reporting, symptoms checking, book an appointment for test, book vaccination appointment	View, write, edit, save, delete (for data stored in HealthNorway)	Data controllers: National Health Registries and HealthNorway for copy	Health Register Act, GDPR, national and international Covid-19 regulations; Full consent to save a copy at HealthNorway
Launching tool catalogue	2019	Citizens can see a list of approved digital health apps and get redirected to use the apps	No data exchange	No shared data processing involved	Basic consent for log in at HealthNorway; Consent in the respective digital health apps

Table A2
Data analysis using Gioia et al. (2013) with quotes.

VERTICAL DATA GOVERNANCE	
Processing data on behalf of healthcare registries	"We [HealthNorway] use the National Institute of Public Health and other official registries to determine access. We have strictly regulated access in HealthNorway, and we use a lot of audit logs for the whole chain to control which actor gets access to HealthNorway and vice versa. And we have login for the citizen, which hospital the citizen is registered at, and if there is established a health contact, that the citizen can contact. So, it is based on a very strict access regime." "For the medication list, they have a right to view it, they do not have a right to get it out. So, you cannot process it for the patient, you can just read it as it is." "HealthNorway is legally grounded in that we get the right consent, the legal consent according to the GDPR, or if not consent, that we have the data processing agreement. […] Based on that the consent models we have, we have the Basic and the Basic Plus and the full consent, which has some services involved to what kind of services you can use." "We were not processing, because the data was in the back-end systems. So, for e-Prescriptions, the data was not stored in HealthNorway. But we could share data with the patient. Just provide a view access." "HealthNorway has the ownership of the data that is processed at HealthNorway and companies or the hospitals are the controllers of the data in their respective systems." "I have been mostly involved in the part that you exchange data with [EPR systems] but also writing secure

(*continued on next page*)

Table A2 (*continued*)

VERTICAL DATA GOVERNANCE	
	text messages through HealthNorway and treating the appointments, then you both write into some part of the EPR and you get things out. So, the reading is one step, writing is one step, that is even a bit harder. So, for example, with Health South East, we have only been able to get the agreements on the reading part, and that was the way to go to get all the rules and agreements on import."
	"The Summary Care Record is a system where the health personnel can log in to access information. What is different from HealthNorway and the Summary Care Record, is that in Summary Care Record, when you log in, you are a health personnel. So, the system will log your activity, and it will make that activity available for patients to see on HealthNorway. But, it also means that if there are cases of misuse or other things happening, then the information cannot be deleted by the inhabitants – like with HealthNorway – it is different. So, systems for use by health personnel need to respect and have different log in ways than systems used by inhabitants."
	"To be able to provide a personalized experience one had to have a data repository and the data repository of [solution] was evaluated to not be fit for that purpose. It was based on a completely different structure and the manageability of it – as far as I remember and at least the way I reflect on it myself – was not appropriate regarding the regulations concerning this type of information."
Storing information on behalf of citizens	"At HealthNorway we store a lot of data on behalf of the citizen which is based on the consent given from the citizen. In some services, we store information on behalf of the sector which is based on an agreement that makes us a processor for the controller who owns the information. And when it comes to data storage outside HealthNorway, we do not have anything to do with that. Outside of HealthNorway is not something that is in production at this point."
	"Information that would be easy to share is information that you as an inhabitant gather and put there [in the HealthNorway storage], because that is your information, there are no other regulations with the third parties or parts of the healthcare system for saving the information there. So, that would be easy. Also, we are saving and storing your preferences regarding how you want the data to be made available. We already have a number of national registries that are using HealthNorway as a storage to save personal information. There is a register, they can have different levels of consent, it is safe [to store] at HealthNorway and the register is accessing that information. If you change it, then we notify the register that: 'This information has now been changed, maybe you have to delete some information'."
HORIZONTAL DATA GOVERNANCE	
	"The patient side, all this information that patients e-mail and the doctors answer, will be stored in the personal health records of the patient. From the doctor's side, this information will be stored in their patient journal systems, so there will be a copy of that dialogue on both sides. That was the motivation for having this personal health archive [at HealthNorway] in place and was the first functionality to be used."
	"GP can get access in HealthNorway, just pick out the one form that s/he needs, which is approved in advance […]. We have the citizen who accepts that: 'I want to be able to share this document with my GP', and that is registered in HealthNorway."
	"There is a video solution provided by Norwegian Health Network [owner of HealthNorway] where we transfer you from HealthNorway into the video solution as you are still authenticated and logged in. That we
Becoming a data controller: exchanging information with healthcare services	also for the GP solutions. For some of the other solutions it is more like a link where we are helping you to access the right video meeting but not sending, or not using your login information."
	"You can just ask for prescription, send questions, and just contact the front desk to ask to change your appointments. Some of the dialogue goes directly to the GP, but some also goes to the health secretary, and some is to ask for a new prescription, that is more automatic. You can also ask questions and start video consultation, and then you also have a tool that helps you to find the right consultant for you – is it best to meet physically, is it best to use the video consultation, or is it okay to just write a question."
	"If the patient is competent to give consent, s/he has to establish the representation himself/herself, and if s/he is not, s/he has dementia, or is not able to understand the consequence of consent, they can have a form filled in that is confirmed by the GP, and we can grant access to the next of kin based on that digital form that confirms it.
	"A copy is stored in HealthNorway, that is the citizen's copy, and the response is sent to the controller who is responsible for maintaining the information they receive due to their legal framework. They have to be in control of how they can use this information – that is the controllers' responsibility."
	"We [HealthNorway] can show what prescriptions you have, but we cannot take that structured data and send it to the GP – that is not part of the regulation. So, we can give you an insight into data, and I am sure you can pull out the structured form of that and send it in an unstructured way to your GP. But, we cannot actually create the solution where it is technically easy to show you prescriptions, see which ones are soon empty, which you need a new prescription for, and send that directly in a structured way to the GP system – that is not
Shared data controlling: structured data generated by citizens	something that is legal to do now. It is technically easy, it will make a lot of sense for citizens and the GPs, but it just requires a change of regulation. "
	"If someone sends you a form, like the Multiple Sclerosis Register, then we transfer you to the form filler of that health register, and that health register will store the form at HealthNorway. But, it will also store it directly in the health register, so you have a copy, and they have their sort of their copy of the information."
	"The Public Health Institute initiated asking the population about their symptoms and they triggered the sending. So, they said 'We want that person to answer this form'. And they [the citizens] would fill in the responses in that form, and HealthNorway would send the forms back to The Public Health Institute. So, that was a service provided to The Public Health Institute by us, and by chance they were using the HealthNorway form filler. "

(*continued on next page*)

Table A2 (*continued*)

VERTICAL DATA GOVERNANCE	
Separate data processing: redirecting citizens to private digital health apps	"That [the digital health apps from the tool catalogue] is available outside of HealthNorway. So, the citizen can choose which tool to use, but the terms of use for that tool are out of our control. It is the agreement from the citizen to the owner of the tool to accept the use of the tool, and how do they process [data] in the tool." "They [the digital health apps from the tool catalogue] have to verify that they follow the Norms for information security in the health sector in Norway. We also have a third-party agreement for being integrated with the Norwegian Health Network, and the 'okay' stamp from Health Directorate that the content is clinically responsible." "The tools that are in the catalogue today are tools that different part of the healthcare sector has said that they want us to make available. For all of the tools we have made a sort of security check that they are compliant with the policies for how to treat and manage data, but it is someone else who has said 'This should be part of the public healthcare offering'. And when there is health information in the tools, then there is some part of the healthcare system that has approved that this is not harming patients 'This is something that we approve of the healthcare part of this tool'."

Table A3
Public document sources.

Document name (translated from Norwegian)	Year	Publisher	Description
Yearly reports (2011-2022)	2011-2022	Norwegian Health Network	12 yearly reports by Norwegian Health Network (owner of HealthNorway since 2020). Describing the digital service needs of actors in the healthcare sector, including HealthNorway functionalities.
One citizen – one record: Digital services in the health and care sector	2012	Ministry of Health	Recommendation to Parliament for patient information to follow the patient lifecycle, and overview of the fragmented IT portfolio in the health and care sector challenging such aspirations.
The primary healthcare service of the future: closeness and comprehensiveness	2015	Ministry of Health	Recommendation to Parliament from the Ministry of Health describing the necessity and importance of the digital dialogue services for GPs and municipalities at HealthNorway.
National health and hospital plan (2016-2019)	2015	Ministry of Health	Recommendation to Parliament from the Ministry of Health describing the necessity and importance of the digital dialogue services with specialist healthcare services at HealthNorway.
Digital citizen services in the specialist health services 2015	2015	National ICT Board	DIS Project for realizing the target image for digital citizen services with one common online health service.
HealthNorway content strategy 2017-2020	2016	Directorate of e-Health	Concrete goals, quality principles and methods for evaluating the quality of the content published at HealthNorway.
Yearly reports (2017-2020)	2017-2020	Directorate of e-Health	4 yearly reports of Directorate of e-Health (owner of HealthNorway until 2019).
Critical health information (alert information) in the Summary Care Record	2018	Directorate of e-Health	Description of principles and guidelines for registering critical information in the national Summary Care Record.
Data responsibilities	2019	Directorate of e-Health	Attachment document explaining data responsibilities for products owned by Directorate of e-Health.
Consultation response Directorate of e-Health: Changes in data responsibility for the Core Summary Care Record, e-Prescriptions, health registries.	2019	Directorate of e-Health	Proposal for changes in legislation and the benefits of a dedicated HealthNorway Act
Guidance in good practice for the use of digital dialogue for GPs	2019	Directorate of e-Health	Advice and recommendations on the technical procedures, facilitation, and further development of the digital dialogue services.
Description of data responsibility for processing personal information in residents' use of services at HealthNorway	2019	Norwegian Health Network	Explaining responsibilities for data processing between HealthNorway and other healthcare actors.
Special Terms of Use for digital citizen services for the Norwegian Board of Health	2020	Norwegian Health Network	These Terms of Use complement HealthNorway – General Terms of Use and provide provisions for the individual services.
Special Terms of Use for digital citizen services for GPs and other health personnel in the primary health service	2020	Norwegian Health Network	These Terms of Use supplement the General Terms of Use of HealthNorway and provide provisions for the primary health services. Primary health services that want to use services at HealthNorway must accept both HealthNorway – General Terms of Use and the special Terms of Use for the relevant services.
Special Terms of Use for digital health and care services for the municipalities	2020	Norwegian Health Network	These Terms of Use supplement the General Terms of Use of HealthNorway and provide provisions for the municipal services. Municipalities that want to use services at HealthNorway must accept both HealthNorway – General Terms of Use and the Special Terms of Use for the relevant services.
Special Terms of Use for patient travel for the Health Trusts' services at HealthNorway	2020	Norwegian Health Network	These Terms of Use supplement the General Terms of Use of HealthNorway and provide provisions for the regional services. Health Trusts that want to use services at HealthNorway must accept both the General Terms of Use of HealthNorway and the Special Terms of Use for the relevant services.

(*continued on next page*)

Table A3 (*continued*)

Document name (translated from Norwegian)	Year	Publisher	Description
Special Terms of Use for the Norwegian Medical Agency's services at HealthNorway	2020	Norwegian Health Network	These Terms of Use supplement the General Terms of Use of HealthNorway and provide provisions for the drug prescription services. Organizations that want to use services at HealthNorway must accept both the General Terms of Use of HealthNorway and the Special Terms of Use for the relevant services.
Special Terms of Use for digital citizen services for the specialist health service	2020	Norwegian Health Network	These Terms of Use supplement the General Terms of Use of HealthNorway and provide provisions for the specialist health services.
HealthNorway product strategy 2021-2026	2020	Norwegian Health Network	Five-year strategy for the development of functionalities and services at HealthNorway.
HealthNorway roadmap	2020	Norwegian Health Network	Addition to the HealthNorway product strategy 2021-2026.
HealthNorway content strategy 2021-2026	2020	Norwegian Health Network	Description of aims for citizen-centric functionalities 2021-2026.
Target architecture for data sharing in the health and care sector	2020	Directorate of e-Health	Describes the need for common components in the digital healthcare services which will facilitate data sharing between data controllers and other health personnel including the patient themselves.
Report of solution concepts: Data sharing infrastructure for digital home follow-up	2020	Directorate of e-Health	Description of alternatives for national data-sharing infrastructure for digital-home follow-up to cover the need of all national, regional, municipal services.
Interim solution for appointment booking of Covid-19 test	2021	Norwegian Health Network	Guide for solution for appointment booking during Covid-19.
Time booking resource	2021	Norwegian Health Network	Guide for GP offices for appointment booking functionality at HealthNorway.
Time booking resource	2021	Norwegian Health Network	Guide for municipalities for appointment booking functionality at HealthNorway.
Temporary staff solution for GPs	2021	Norwegian Health Network	Guide for the usage of digital dialogue functionalities by temporary staff.
Digital forms at HealthNorway	2021	Norwegian Health Network	Overview of common components and functionalities related to the digital form services at HealthNorway.
General Terms of Use for HealthNorway	2021	Norwegian Health Network	Terms of Use regulating general provisions that apply to all companies that use services at HealthNorway.
HealthNorway – Terms of Use for vendors	2021	Norwegian Health Network	The Terms of Use for all integrations and technical interfaces between the external solution and the national e-health solutions that are in production.
Collaboration with industry in the e-health area	2021	Directorate of e-Health	Recommendations and principles for collaborating with actors from the industry.
Prescription of tools via the tool broker	2022	Norwegian Health Network	User guide for citizens and healthcare personnel in prescribing digital health tools.
Safer health apps	2022	Directorate of Health	Proposal for a national evaluation framework and model for usage of private digital health apps.
Assessment of principles for connection between HealthNorway and other solutions in the market	2022	Directorate of e-Health	Principles for providing seamless experience for citizens to use regional and municipal digital health services which interact with HealthNorway.

References

Aaltonen, A., Alaimo, C., & Kallinikos, J. (2021). The making of data commodities: Data analytics as an embedded process. *Journal of Management Information Systems, 38*(2), 401–429.

Aanestad, M., Jolliffe, B., Mukherjee, A., & Sahay, S. (2014). Infrastructuring work: Building a state-wide hospital information infrastructure in India. *Information Systems Research, 25*(4), 834–845.

Abbasi, A., Sarker, S., & Chiang, R. (2016). Big data research in information systems: Toward an inclusive research agenda. *Journal of the Association for Information Systems, 17*(2), 1–32.

Abraham, R., Schneider, J., & vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management, 49*, 424–438.

Alaimo, C., Kallinikos, J., & Aaltonen, A. (2020). In *Data and value. Handbook of digital innovation* (pp. 162–178). Edward Elgar Publishing.

Alvesson, M., & Sköldberg, K. (2010). *Reflexive methodology: New vistas for qualitative research* (Vol. 12). Routledge.

Bardhan, I., Chen, H., & Karahanna, E. (2020). Connecting systems, data, and people: A multidisciplinary research roadmap for chronic disease management. *MIS Quarterly, 44*(1), 185–200.

Benfeldt, O. (2017). A comprehensive review of data governance literature. *Selected Papers of the IRIS*, 120–133.

Benfeldt, O., Persson, J. S., & Madsen, S. (2020). Data governance as a collective action problem. *Information Systems Frontiers, 22*(2), 299–313.

Berends, H., & Deken, F. (2021). Composing qualitative process research. *Strategic Organization, 19*(1), 134–146.

Bonina, C., & Eaton, B. (2020). Cultivating open government data platform ecosystems through governance: Lessons from Buenos Aires, Mexico City and Montevideo. *Government Information Quarterly, 37*(3), Article 101479.

Bowker, G. C., Baker, K., Millerand, F., & Ribes, D. (2009). Toward information infrastructure studies: Ways of knowing in a networked environment. In J. Hunsinger, L. Klastrup, & M. Allen (Eds.), *International handbook of internet research* (pp. 97–117). Netherlands: Springer.

Constantinides, P., & Barrett, M. (2015). Information infrastructure development and governance as collective action. *Information Systems Research, 26*(1), 40–56.

Constantiou, I. D., & Kallinikos, J. (2015). New games, new rules: Big data and the changing context of strategy. *Journal of Information Technology, 30*(1), 44–57.

Corley, K. G., & Gioia, D. A. (2011). Building theory about theory building: What constitutes a theoretical contribution? *Academy of Management Review, 36*(1), 12–32.
DalleMule, L., & Davenport, T. H. (2017). What's your data strategy. *Harvard Business Review, 95*(3), 112–121.
Directorate of e-Health. (2021). *Collaboration with industry in the e-health area*.
European Commission. (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). *Official Journal of the European Union, 59*(1), 1–88.
European Commission. (2020). *Communication from the commission to the European Parliament*. The Council, The European Economic And Social Committee And The Committee Of The Regions A European strategy for data.
Fadler, M., Lefebvre, H., & Legner, C. (2021). Data governance: From master data quality to data monetization. *ECIS 2021 Research Papers*, 16.
Fadler, M., & Legner, C. (2020). Who owns data in the enterprise? Rethinking data ownership in times of big data and analytics. *ECIS 2020 Proceedings*, 17.
Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. *Organizational Research Methods, 16*(1), 15–31.
Greengard, S. (2018). Weighing the impact of GDPR. *Communications of the ACM, 61*(11), 16–18.
Grisot, M., Hanseth, O., & Thorseng, A. (2014). Innovation of, in, on infrastructures: Articulating the role of architecture in information infrastructure evolution. *Journal of the Association for Information Systems, 15*(4), 197–219.
Jagals, M., & Karger, E. (2021). Inter-organizational data governance: A literature review. *ECIS 2021 Proceedings*, 20.
Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., & Janowski, T. (2020). Data governance: Organizing data for trustworthy artificial intelligence. *Government Information Quarterly, 37*(3), Article 101493.
Khatri, V., & Brown, C. V. (2010). Designing data governance. *Communications of the ACM, 53*(1), 148–152.
Lee, S. U., Zhu, L., & Jeffery, R. (2017). Data governance for platform ecosystems: Critical factors and the state of practice. *PACIS 2017 Proceedings*, 12.
Markus, M. L., & Bui, Q. N. (2012). Going concerns: The governance of interorganizational coordination hubs. *Journal of Management Information Systems, 28*(4), 163–198.
Nokkala, T., Salmela, H., & Toivonen, J. (2019). Data governance in digital platforms. *AMCIS 2019 Proceedings*, 10.
Otto, B. (2011). Organizing data governance: Findings from the telecommunications industry and consequences for large service providers. *Communications of the Association for Information Systems, 29*.
Parmiggiani, E., & Grisot, M. (2020). Data curation as governance practice. *Scandinavian Journal of Information Systems, 32*(1), 3–38.
Rosenbaum, S. (2010). Data governance and stewardship: Designing data stewardship entities and advancing data access: Data governance and stewardship. *Health Services Research, 45*(5p2), 1442–1455.
Star, S. L., & Ruhleder, K. (1994). Steps towards an ecology of infrastructure: Complex problems in design and access for large-scale collaborative systems. In *Proceedings of the 1994 ACM conference on computer supported cooperative work - CSCW '94* (pp. 253–264).
Susha, I., Janssen, M., & Verhulst, S. (2017). Data collaboratives as "bazaars"?: A review of coordination problems and mechanisms to match demand for data with supply. *Transforming Government: People, Process and Policy, 11*(1), 157–172.
Tallon, P. P., Ramirez, R. V., & Short, J. E. (2013). The information artifact in IT governance: Toward a theory of information governance. *Journal of Management Information Systems, 30*(3), 141–178.
Van Alstyne, M., Brynjolfsson, E., & Madnick, S. (1995). Why not one big database? Principles for data ownership. *Decision Support Systems, 15*(4), 267–284.
Van den Broek, T., & Van Veenstra, A. F. (2015). Modes of governance in inter-organizational data collaborations. *ECIS 2015 Proceedings*, 13.
Vassilakopoulou, P., Skorve, E., & Aanestad, M. (2019). Enabling openness of valuable information resources: Curbing data subtractability and exclusion. *Information Systems Journal, 29*(4), 768–786.
Vilminko-Heikkinen, R., Brous, P., & Pekkola, S. (2016). Paradoxes, conflicts and tensions in establishing master data management function. ECIS 2016 Proceedings. 184.
Viljoen, S. (2021). A relational theory of data governance. *Yale LJ, 131*, 573.
Weill, P., & Ross, J. W. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business Press.
Winter, J. S., & Davidson, E. (2019). Big data governance of personal health information and challenges to contextual integrity. *The Information Society, 35*(1), 36–51.
Winter, J. S., & Davidson, E. J. (2020). Harmonizing regulatory spheres to overcome challenges for governance of patient-generated health data in the age of artificial intelligence and big data. In *TPRC48: The 48th research conference on communication, information and internet Policy*.
Zhang, Q., Sun, X., & Zhang, M. (2022). Data matters: A strategic action framework for data governance. *Information & Management, 59*(4), Article 103642.