Designing for Trust in Healthcare Data Sharing: Trust Anchors in the Trust Framework Lifecycle

Louise van der Peet(✉), Wendy van Donge, Nitesh Bharosa, and Marijn Janssen

Delft University of Technology, Delft, The Netherlands
l.vanderpeet@tudelft.nl

Abstract. Trust is a crucial factor in multi-actor data-sharing initiatives, particularly in sensitive domains like healthcare, where patient privacy, regulatory requirements, and organizational collaboration intersect. However, achieving trust-by-design, creating trust through intentional design choices, is challenging. To address this challenge, this paper investigates how trust frameworks in healthcare data-sharing are designed and how they evolve over time. Central to this inquiry is the conceptualization of "trust anchors"– designable components that provide a foundation for creating trust. Drawing on Technological Innovative Systems theory, this research qualitatively examines two healthcare trust frameworks, each at different lifecycle stages. The case studies reveal how trust anchors contribute to both the development and active management of trust frameworks. The contribution includes a lifecycle approach for trust frameworks and a matrix for categorizing trust anchors, providing guidance for organizations aiming to implement and maintain multi-actor data-sharing frameworks. We find that enforceable trust anchors are more important in the mature phase of a trust frameworks, while in the growing phase, less designable and enforceable trust factors assume a greater role.

Keywords: Data sharing · Trust Frameworks · Trust · Technological Innovation System Theory · GovTech

1 Introduction

Sharing healthcare data among multiple organizations has the potential to improve patient outcomes drastically, reduce costs, and foster innovation [18]. However, sharing (sensitive) data is challenging because all participating stakeholders must have trust in both the systems and actors. Even with state-of-the-art technical safeguards, stakeholders may still doubt each other's motives, business models, data quality, and commitment to privacy. This tension highlights the duality of trust in healthcare data-sharing initiatives: it is both technical and social, requiring both a secure infrastructure and confidence in the relationships, governance, and values binding participating organizations.

Published by Springer Nature Switzerland AG 2026
I. Lindgren et al. (Eds.): EGOV 2025, LNCS 15944, pp. 150–163, 2026.
https://doi.org/10.1007/978-3-032-01589-1_10

To address these complexities, public-private trust frameworks have emerged as a GovTech steering instrument for aligning public and private actors in multi-actor data sharing collaborations. GovTech is the umbrella term for digital systems and services that private companies develop and operate to streamline and support public-sector work [4]. By defining shared rules, standards, and processes, trust frameworks aim to ensure that each stakeholder can trust that all participants comply with collaborative agreements. However, designing such a socio-technical system can be complex. Rather than being a one-off implementation, the framework goes through a continuous process, beginning with initial agreements that establish a basic foundation, and then evolving through updates, re-evaluations, and the incorporation of new technologies and stakeholders. This ongoing development means that different trust factors may become relevant in various phases, due to changing needs and requirements.

We propose that trust in a trust framework is created through certain "trust anchors". While the literature offers numerous definitions of trust anchors, we adopt a generic definition that broadly encompasses many of these existing definitions: designable components providing a shared foundation for trust creation. Examples from the literature include trust anchors as an architectural solution for trust establishment in 6G networks [17], the association of a DNSSEC trust point name with a public key [1], an authoritative entity for which trust is assumed [14], and a hardware-assisted dynamic root of trust [6].

Because they can be intentionally created and deployed, trust anchors can be particularly useful for organizations seeking to arrange for data-sharing in a multi-actor environment. Our premise is that the more knowingly actors design and implement trust anchors, the faster they can move from pilot programs toward mature frameworks.

However, there is a gap in our understanding of which trust anchors matter most and when, and how the role of public organizations evolves during this process. To explore this, we take a lifecycle perspective drawn from Technological Innovation Systems (TIS) theory [13], examining how trust in healthcare data-sharing collaborations evolve from early formation to operational maturity. In particular, we focus on how trust anchors evolve, and how involvement of public organizations changes over time in trust frameworks. With public agency involvement we refer to the extend with which governmental or publicly mandated organizations shape, fund, or oversee a trust framework's design and governance. We aim to answer the following research questions:

RQ1. What are necessary trust anchors in different phases of trust framework design?
RQ2. How does public agency involvement evolve during the phases of a trust framework?

We qualitatively analyze two healthcare trust frameworks that are each in a different lifecycle phase: growth and maturity. Through semi-structured interviews, we identify which trust factors participants see as essential, compare these factors to known antecedents of trust in trust frameworks, and examine the evolving nature of public agency involvement.

The remainder of this paper is organized as follows. First, we lay out the theoretical foundations related to TIS lifecycles. We then describe the qualitative research approach and the two case studies in detail. Next, we present our findings on different trust anchors and public agency involvement as the frameworks evolve. Finally, we discuss implications for the design and development of trust frameworks.

2 Theoretical Background

2.1 Technological Innovation System Lifecycle for Trust Frameworks

To investigate how trust frameworks evolve and identify the key trust factors, we need an applicable lifecycle perspective. Since there is no lifecycle theory specifically for trust frameworks, we draw instead on a related theory: technological innovation system theory.

A technological innovation system (TIS) can be seen as a network of interconnected actors and institutions that collaborate within a specific technological domain. Together, they generate, disseminate and implement a new variant of technology or product [3,13]. Although the TIS framework has been used primarily in research on sustainability transitions [2], it is also applicable to trust frameworks, such as these collaborations between actors in a technological domain who implement a new variant of a technology or standardization. In this study, we focus on the lifecycle of TIS, which consists of stages of formation, growth, maturity, and decline [13]. We discuss the growth and maturity phase in more depth, as they are relevant for the research. A summary of all phases can be found in Fig. 1.

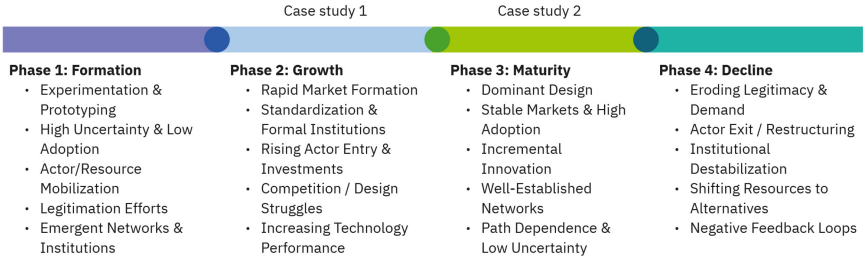

Fig. 1. Technological Innovation Systems phases based on [13]

In the growth phase, the TIS becomes more defined and structured. Technology-specific institutions, such as standards, gain influence, and market formation begins with emerging value chains and dominant designs guiding development. Relationships within the system also expand, meaning the TIS not only depends on its context but also actively shapes it. These connections

include producerâĂŞsupplier ties, customer relationships, and links with complementary systems, which together create a complex web of inter-dependencies that can be both cooperative and competitive.

In the mature phase, a Technological Innovation System is highly institutionalized, with stable, well-established structures and a large amount bidirectional relationships. Although major changes are rare, incremental adaptation does occur, and the technology can gradually extend into new application areas.

Even though trust framworks fit well in the concept of Technological Innovation System theory, there are some limitations to the approach. TIS focuses on technical systems, rather than socio-technical systems like a trust framework. In that world, progress is measured by R&D spending, patent counts and economies of scale. This means there is more focus on the technology than on other important aspects of trust frameworks like governance or policy. TIS also focuses on unidirectional and bidirectional relationships, while trust frameworks are often related to network relationships.

3 Research Approach

Healthcare data-sharing initiatives present unique complexities, given the sensitivity of the information exchanged, the variety of stakeholder interests, and the challenges of privacy and security. This study adopts a case-based research approach to investigate trust's evolving role as trust frameworks progress, as it remains unclear which trust factors are most relevant at which point in a trust framework's lifecycle, and how public agency involvement evolves.

Existing research on trust lifecycles in business relationships shows that mature relationships often require more designable and enforceable trust, and growing relationships rely on less formal trust mechanisms. For example, Dowell et al. [8] found that emotional trust is more important in early stages of business-to-business relationships, and cognitive trust becomes more important in the mature phase. Similarly, Heffernan [11] finds that in cross-cultural business-to-business relationships, trust initially relies more on reputation, then contractual and competence trust, and later includes goodwill trust. We believe this could also be the case for trust frameworks, because the initial phase requires actors to work more together and trust eachother, requiring more relational trust, and the later stages rely more on the trustworthiness of the system. In other words: enforceable trust anchors become more important in the mature stage of a trust framework.

Furthermore, as GovTech solutions gain popularity, public organizations are evolving from regulatory or funding bodies into direct co-creators of socio-technical solutions [5]. Examining how their role develops in public-private trust frameworks offers deeper insight into the lifecycle of trust frameworks–revealing how, through GovTech, these organizations become both regulators and active participants in the co-design of digital systems.

To answer the research questions involving which trust anchors arise in different phases of a trust framework's lifecycle and how public agency involvement

evolves, we conducted semi-structured interviews for two trust frameworks: the first for reporting accountability information in a health care setting and the second for certifying personal health record systems. Each represents a different phase of development (respectively growth and maturity). We have chosen not to include the formation and decline phase for practical reasons. The formation phase typically requires a longer, longitudinal approach since it is not yet clear whether a given initiative will evolve into a fully established trust framework. Furthermore, because trust frameworks are a relatively recent concept, no known examples are currently in the decline phase.

For each of the two cases, we interviewed a case expert. Yin [19] points out that case studies are highly suitable for exploring current phenomena in their natural context. Likewise, Eisenhardt [9] suggests that examining a small number of cases can be a useful approach for developing theoretical insights. Semi-structured interviews follow a predetermined thematic framework, but still allow for an in-depth exploration of topics that arise through the open-ended responses. This allows the interviewees freedom to explain their thoughts and highlight which topics are important to them, with less input from the interviewer [12]. In the interviews we asked about trust factors; given that it is a broad topic with many different answers, this gave the interviewee space to discuss what they think is most important. The interview consisted of two parts: (1) a discussion of the case itself, describing the trust framework and public/private sector involvement, and (2) an exploration of factors influencing trust. We used purposive sampling, selecting one of the leading experts from each trust framework for the interviews. The selection criteria for these respondents included their extensive involvement in the design, implementation, and management of the trust framework. We chose one respondent per case to ensure that we captured a focused, expert perspective from those who are directly responsible for shaping and sustaining the framework. In addition to the interviews, we also consulted the official documentation for each trust framework to verify and elaborate our findings.

The interviews were audiotaped, transcribed, and validated by the respective interviewees, then uploaded to ATLAS.ti for qualitative coding. The interview questions can be requested through the authors. The data was anonymized to remove any personally identifiable information. We used deductive coding to analyze the interview, applying pre-identified trust antecedents [15] as our coding framework. Due to page restrictions the appendeces from this paper were removed, these are available upon request. This deductive approach was chosen over an inductive one to test and validate existing theoretical constructs in a structured manner. To ensure that we did not overlook any potential new variables, we kept an open perspective during the coding process, allowing for the identification of unexpected trust factors.

There are some limitations to this research method. First, only a small number of case studies and participants were involved, which may limit the generalizability of the findings. Moreover, both case studies originate from the Netherlands, which could limit results to that cultural and regulatory setting.

4 Forms of Trust Frameworks in Healthcare: Case Descriptions

In this section, we present the two healthcare trust framework cases that illustrate different phases of the TIS lifecycle. As shown in Fig. 1, the first case is in the growth phase, while the second has reached the mature phase.

4.1 Case Study 1: Reporting Accountability Information in a Health Care Setting

In the Netherlands, healthcare professionals spend an increasing amount of time on administrative tasks and the shortage of healthcare professionals is expected to worsen in the coming years [10,16]. Professionals need to be able to focus on the core of their tasks, rather than administrative burdens. To address these challenges, it is crucial to reduce the administrative load, and one solution is to improve the efficiency of health care reporting. In the first case study, a trust framework was introduced to standardize healthcare accountability reporting to streamline the reporting process. This approach aims not only to reduce administrative burdens, but can also increase the quality of the shared information.

A central principle of this project is the reuse of pre-existing data. By using an ontology for standardization, the same data can be applied to answer various accountability information requests from different parties. Reuse is particularly important here; in the initial phase, a review was conducted to assess the data that was already available from internal business processes, in the ontology, this data is repurposed. In this manner, the healthcare organization does not have to compile or collect new data, and the standardized dataset remains at the source. The healthcare provider compiles the answers from the dataset and shares them with the appropriate recipients. Because every question is answered using the same dataset and the ontology is standardized in the chain, the quality and comparability of the answers improve, while minimizing the administrative effort required from the healthcare provider.

The trust framework is in the growth phase of its lifecycle. Starting with pilots in nursing home, it is now expanding towards more sectors in the healthcare domain. An expanding group of participants, beyond the early adopters, is now involved, supported by a formal governance structure (including strategic and tactical consultations, as well as a management organization). Standardization efforts are being put into practice and are gaining traction as more actors come on board, with participating actors adapting their datasets to align with the framework's standards.

Trust Factors. The participant in this case study identified several factors that influence trust in the system. Many of these fell under the calculative trust category: benefit by improved information position or incentives for trust framework participants, the importance of adoption by partners and competitors, low costs, and the applicability of the standardization to multiple objectives. The participant compares trust framework adoption to that of electric vehicles:

> "Nobody's going to buy that kind of car if there aren't any charging stations to charge it, or if it's a lot more expensive than regular cars. And there won't be any charging stations if there aren't enough cars on the road. So you have to try to get things off the ground on both sides, knowing that it only truly improves when as many parties as possible join in. Because until then, it's not actually better; it's just more expensive, more tedious, and different."

Notably, low costs and multi-purpose applicability were not observed in the prior study on trust factors. Having low costs can be specifically important for particular healthcare organizations, as they are often publicly funded or non-profit and budgets for innovation can be low. Additionally, the participant mentioned that trust can strengthen if the change that is made for innovation is applicable to multiple goals, e.g. if the change in the database will also make it easier to manage the data; or if the standardization of data will make it more usable for more objectives like scientific research.

Under the technical trust category, privacy, security, technical compatibility, data governance, and perceived usefulness were mentioned as important factors to trust. However, the participant mentions that these are not the most important factors:

> "I think [the participants] tend to focus more on whether it fits within the current landscape, whether it doesn't cost too much money, and whether it doesn't require extra effort. I haven't really heard them discuss the actual underlying agreements".

In this growth phase of the trust framework, practical considerations such as cost-effectiveness, alignment with existing systems, and broad adoption are deemed important. Factors like low cost and multi-purpose applicability underline the importance of immediate benefits and ease of integration during early adoption. The designable trust anchors we identified in this phase are: Ease of use, Multi-purpose applicability, Technical compatibility, Low costs, Privacy, Security and Data governance. In the discussion we will further explain the classification of trust anchors.

Public Agency Involvement. In this trust framework, no direct agreements are made with private organizations. Instead, agreements are indirectly translated to the healthcare providers through other channels. The framework is managed by a governmental organization. Additionally, a higher level governmental body (of policy organization) provides financing. While healthcare organizations do not directly participate in the governance, their interests are represented through branch organizations. They provide input for the public sector on which to base the decision-making. The participant mentions that this public-private division is not fixed and may evolve over time. It is important to mention that the participant notices there are private organizations with a public task and public funding in the governance. However they are there to represent the governmental organizations, so they are considered public.

4.2 Case Study 2: Certifying Personal Health Record Systems

Patient health data are sensitive by nature, making the healthcare sector a major target for information theft. The response by healthcare providers has often resulted in reduced accessibility of data for patients and collaborating healthcare providers [7].

To address this challenge, healthcare organizations in the Netherlands are working with personal health record systems to enable the safe sharing of medical information between patients and healthcare providers. Central to this approach is a trust framework that establishes rules for the secure and trustworthy exchange of health data. Organizations that participate must comply with these rules to obtain a specific label, which serves as an assurance that health data is managed and shared according to strict security and privacy standards. In addition, this framework allows patients to view, manage, and share their health data in one centralized location. By ensuring that both patients and providers are well informed through secure data practices, the system aims to support improved healthcare data accessibility and security.

This trust framework can be viewed as operating in the mature phase. It has become highly institutionalized, indicated by government involvement, and the presence of a managing foundation. The governance structure is stable, and little significant changes to standards are made, indicating that the framework has reached an established state of implementation.

Trust Factors. The participant in this trust framework placed more emphasis on its institutionalization. In institution-based trust, both the connection to regulations, and oversight were mentioned as important trust anchors. Connecting a trust framework to existing regulations, or creating new regulations around it increases the assurance of actors fulfilling agreements; otherwise there will be legal consequences. Oversight similarly ensures that any agreements are effectively enforced. As the participant points out, this enforcement could be formalized in laws or regulations:

> "The systems of individual healthcare providers are much less secure than [those that meet the requirements of the trust framework]. But who actually enforces that those systems should also meet a higher security standard? You could, of course, lay down that enforcement in the law."

Cryptography is also mentioned as an important anchor, suggesting that regulating organizations should provide guidance on what constitutes an acceptable or "state-of-the-art" standard. As the respondent noted, it would be beneficial if regulators could specify standards that they consider state-of-the-art, for example, recommending the use of multiparty computation or synthetic data. This could assure stakeholders that a particular cryptographic implementation is acceptable, even if achieving these standards requires additional time and resources.

Under organizational competence, the participant highlighted the need for a stable organizational structure, including steady finance and job security. These

factors go hand-in-hand: a trust framework requires reliable funding, and short-term subsidies create insecurities around employment. Again, linking the framework to regulation could help, providing structural financing from public organizations:

> "You need this for continuity: if it is stated by law that you are assigned legal duties, then structural funding will be connected. That means money, and it also affects employment."

Regarding relational trust, the participant emphasizes effective collaboration and open communication. They specifically mentioned procedural transparency, inclusion and collaborative decision-making as important elements in the governance:

> "It's easier if one party just acts like a dictator and says, 'this is how we're going to do it.' When people eventually get fed up with endless discussions, they forget that before, they weren't allowed to do or decide anything at all. Now there might be too much consultation, and they start thinking, 'Let's make this easier: let's just have one party decide.' But that indeed comes at the expense of both trust and legitimacy."

Overall, the participant strongly emphasized the role of regulation in ensuring a mature trust framework. Legal anchoring not only enforces compliance and provides clarity on technical matters (such as cryptography), but also lays a foundation for stable funding and job security. As trust frameworks evolve, regulatory support appears to become an increasingly critical factor, creating continuity, accountability and legitimacy. It is interesting that all of these factors can be considered trust anchors, as they are all designable.

Public Agency Involvement. One of the goals of this trust framework is to ensure that public values are upheld in personal health record systems. This emphasis on public values means that public agency involvement is a critical part of the framework, ensuring that these sensitive platforms are not only in control of Big Tech platforms.

The participant explains that the role of public organizations shifts throughout the lifecycle of the trust framework. In the formation and growth phases, the governance structure was evenly divided between public and private actors. For example, the participant council, which includes ICT suppliers of personal health record systems, played a more important role during the early stages. When a new release was proposed, it had to pass through the participant council; if they disagreed, this carried a considerable weight. As the framework matured and the number of participants increased, it became impossible to consider everyone's opinion, and the participant council's influence gradually diminished. While their input is still taken into account, it is more dependent on well-founded arguments.

Initially, the know-how of the private organizations was more important. Over time, as more actors joined the collaboration, considering all opinions became

more challenging. Public debates also influenced this shift, with a growing consensus that government should take more control in managing healthcare data. The participant mentioned that the government is now inclined to take charge of everything, while taking control does not necessarily mean handling everything alone.

Taking all this into account, the participant highlighted the difficulty in clearly distinguishing between public and private organizations within the healthcare sector. In this context, the government is considered public and organizations such as health insurance providers, general practitioners, and the patient federation are considered private. However, most stakeholders operate in the public domain and the division between the public and the private sector is more nuanced.

5 Discussion

Our research focuses on two questions related to the lifecycle of trust frameworks: do different trust anchors emerge at different stages, and does the role of public agency involvement evolve along with these stages? Our aim in defining trust anchors is to simplify the design process by highlighting which areas offer the greatest impact in each phase. However, it is important to acknowledge that not all trust factors can be directly designed. We use trust factors as the umbrella term for all attributes that shape stakeholders' willingness to rely on a socio-technical system. Trust anchors are the subset of those factors that satisfy three conditions: they can be intentionally specified ex-ante by the governing bodies and their presence can be verified or audited with reasonable objectivity. By contrast, emergent trust factors (such as reputation and shared values) tend to develop organically and are inherently more challenging to create intentionally. Some attributes overlap the categories. Procedural transparency meets the criteria for trust anchors; perceived transparency, however, depends on the interpretation of actors and is more like an emergent factor.

Our findings indicate that different types of trust anchors occur in the two lifecycle phases. In the growth phase, trust relies more on emergent, relational factors, anchors that arise from collaboration and shared values. More formal, intentionally designed, and enforceable trust anchors were seen as important in the mature framework. To better understand this shift, we examine whether a given trust factor is susceptible to deliberate design or formal enforcement.

To systematically capture these distinctions, we developed a classification matrix that maps trust factors along two dimensions: designability and enforceability (see Fig. 2). By designability, we refer to how deliberately a given trust factor can be conceived, structured, or otherwise engineered by those creating the framework. These designable factors are also referred to as trust anchors. The enforceability dimension measures the extent to which adherence to a trust factor can be mandated or ensured. Factors high in enforceability can be monitored and penalized if violated (e.g., security certifications), whereas less enforceable factors rely on voluntary compliance or social norms. Mapping trust factors on

these dimensions allows us to differentiate between those that can be built into the system's design and those that require external checks and balances, which can help researchers and organizations think in terms of more engineerable and maintainable trust.

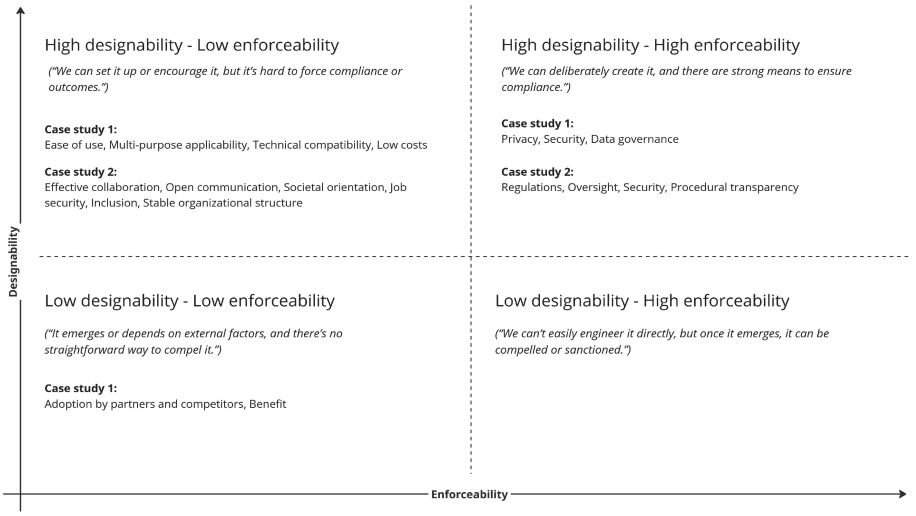

Fig. 2. Trust antecedents matrix: designability and enforceability

The diagram in Fig. 2 reveals that in the growth phase of a trust framework, observed in the first case study, there is a greater reliance on factors that are low in both designability and enforceability. In contrast, the second case, which is in the mature phase, contains only factors that are high in designability: trust anchors. This suggests that as trust frameworks evolve, there is a natural progression where the importance of low designable and low enforceable trust factors shifts to those that can be deliberately designed and enforced. The design proposition derived from our research is as follows:

> In the growing phase of a trust framework, reliance on less designable and enforceable trust factors is more prominent, whereas in the mature phase, designable and enforceable anchors become important.

The type of trust anchors is not only dependent on the stage in the lifecycle, trust anchors are indispensable in all phases of the cases we researched. The more that is understood about trust anchors, the more active designing is possible, and this can accelerate the lifecycle progression.

The analysis of public agency involvement across our two case studies reveals different patterns that do not clearly align with the lifecycle perspective. In one case, public agency involvement is already large in the growth phase, with

agreements and oversight predominantly managed by governmental organizations, while private actors are represented through branch organizations. In the other case, there is a clear shift towards more public agency involvement in the mature phase. These contrasting findings suggest that the relationship between public agency involvement and the trust framework lifecycle is not evident, and no definitive conclusion can be drawn regarding a consistent evolution of public-private roles over time.

From a theoretical perspective, this study applies and extends Technological Innovation Systems (TIS) theory by highlighting how trust frameworks in healthcare evolve through growth and maturity phase, yet often involve complex socio-technical interactions not fully captured by the TIS lifecycle model. Specifically, we introduce "trust anchors" as designable components that help accelerate progression through these phases, showing that certain trust factors (low in designability and enforceability) typically dominate early on, while more designable elements, also known as trust anchors, become central in later stages.

On a practical level, our proposed classification matrix (Fig. 2) offers actionable guidance for organizations aiming to implement or improve trust frameworks. By distinguishing between elements that can be easily designed or enforced and those that rely on more emergent, relational processes, stakeholders can prioritize resources to their stage of development. Public-sector agencies can treat the matrix's designable anchors as leading indicators for project managers and use the emergent anchors to estimate overall maturity, while policymakers can benchmark the framework's progress through the same matrix, informing how they allocate resources and phasing legislative or supervisory measures in line with the framework's evolution.

While these findings offer valuable insights, there are some limitations. Specifically, the small number of participants per case study and the limited number of case studies constrain the generalizability of the findings. Additionally, both of these case studies are situated in The Netherlands, which may limit cross-cultural applicability, as well as cross-regulatory applicability. Furthermore, the findings on public agency roles over time are less conclusive. In future studies, more case studies can be performed to test the design proposition, and more factors that influence the need of certain trust factors can be tested, like sectoral affiliation, data sensitivity and risk profile, the regulatory environment, and stakeholder diversity. Future work could include a longitudinal study on trust anchors, to get a better understanding of how they develop and how trust in this setting evolves over time. Additionally, extra case studies could provide a more in-depth picture of the evolution of public agency involvement in trust frameworks.

6 Conclusion

This paper examined how trust anchors in healthcare data-sharing trust frameworks progress over time and how public agency involvement changes within these collaborations. We introduced the concept of trust anchors as deliberately

designable components that provide a foundation for trust. Through two case studies, one in the growth phase and another in the mature phase, we found that different trust anchors are important in each stage.

In response to RQ1, we found that in the growth phase, less designable and enforceable trust factors are more influential. As for trust anchors, practical considerations and anchors for immediate benefits, such as low costs and technical compatibility are seen as important. In the mature case study, enforceable trust anchors are more important, with a clearer focus on institutionalization, with trust anchors such as regulations and oversight; this legal anchoring can create continuity, accountability and legitimacy in the later stages of the trust framework. Ultimately, the growth phase focuses on practical, readily implementable factors to boost adoption, whereas the mature phase relies on formal, enforceable mechanisms to create or maintain trust.

For answering RQ2, regarding public agency involvement, both trust frameworks exhibited substantial governmental participation regardless of maturity level. This could be indicative for the healthcare sector: a sector that generally has large public agency involvement. We therefore found no significant difference in public agency involvement across these two phases of trust framework evolution.

Overall, these findings underscore the importance of aligning trust anchors with a framework's stage of development. Future work could expand on this research by examining more case studies to see how different organizational contexts, technologies, and policy environments shape the interplay between trust anchor design and public agency involvement in data-sharing collaborations.

References

1. Aust, R., Larson, M., Massey, D., Rose, S.: Rfc 5011: Automated updates of dnssec trust anchors. RFC 5011, Internet Engineering Task Force (2007). https://www.rfc-editor.org/rfc/rfc5011.txt. Accessed 18 Feb 2025
2. Bergek, A.: Technological innovation systems: a review of recent findings and suggestions for future research. In: Handbook of Sustainable Innovation, pp. 200–218 (2019)
3. Bergek, A., Hekkert, M., Jacobsson, S., Markard, J., Sandén, B., Truffer, B.: Technological innovation systems in contexts: conceptualizing contextual structures and interaction dynamics. Environ. Innov. Soc. Trans. **16**, 51–64 (2015)
4. Bharosa, N.: The rise of govtech: trojan horse or blessing in disguise? A research agenda. Gov. Inf. Q. **39**(3), 101692 (2022)
5. Bharosa, N., van Wijk, R., de Winne, N.: Challenging the Chain: Governing the Automated Exchange and Processing of Business Information. IoS Press (2015)
6. Brasser, F., El Mahjoub, B., Sadeghi, A.R., Wachsmann, C., Koeberl, P.: Tytan: tiny trust anchor for tiny devices. In: Proceedings of the 52nd Annual Design Automation Conference, pp. 1–6 (2015)
7. Dagher, G.G., Mohler, J., Milojkovic, M., Marella, P.B.: Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustain. Cities Soc. **39**, 283–297 (2018)

8. Dowell, D., Morrison, M., Heffernan, T.: The changing importance of affective trust and cognitive trust across the relationship lifecycle: a study of business-to-business relationships. Ind. Mark. Manag. **44**, 119–130 (2015)
9. Eisenhardt, K.M.: Building theories from case study research. Acad. Manag. Rev. **14**(4), 532–550 (1989)
10. FNV: Onderzoek– zorg- & welzijnsbarometer (2024). https://www.fnv.nl/getmedia/00206470-8f1f-4ae1-9fc8-9a8f9a7d40be/FNV-Zorg-en-Welzijnsbarometer-rapportage-n-a-v-onderzoek-adminstratiedruk-in-de-sector-Zorg-en-Welzijn-mei-2024.pdf. Accessed 19 Feb 2025
11. Heffernan, T.: Trust formation in cross-cultural business-to-business relationships. J. Cetacean Res. Manag. **7**(2), 114–125 (2004)
12. Horton, J., Macve, R., Struyven, G.: Qualitative research: experiences in using semi-structured interviews. In: The Real Life Guide to Accounting Research, pp. 339–357. Elsevier (2004)
13. Markard, J.: The life cycle of technological innovation systems. Technol. Forecast. Soc. Chang. **153**, 119407 (2020)
14. National Institute of Standards and Technology: Trust anchor (nd). https://csrc.nist.gov/glossary/term/trust_anchor. Accessed 18 Feb 2025
15. van der Peet, L., Bharosa, N., Janssen, M.: From trust antecedents to trust frameworks: Co-creating multi-actor agreements for data sharing. In: Conference on Digital Government Research, vol. 1 (2025)
16. Research, A.: Arbeidsmarktprognoses zorg en welzijn (2024). https://abfresearch.nl/cases/arbeidsmarktprognoses-zorg-en-welzijn/. Accessed 19 Feb 2025
17. Veith, B., Krummacker, D., Schotten, H.D.: The road to trustworthy 6g: a survey on trust anchor technologies. IEEE Open J. Commun. Soc. **4**, 581–595 (2023)
18. World Health Organization: Global Strategy on Digital Health 2020–2025. World Health Organization (2021). https://apps.who.int/iris/handle/10665/311980, available under the CC BY-NC-SA 3.0 IGO license
19. Yin, R.K.: Case study research: Design and methods, vol. 5. sage (2009)