ISSN: 2754-6659

Journal of Artificial Intelligence & Cloud Computing

SCIENTIFIC Research and Community

Review Article

Open Access

Bridging the Data Divide: Secure Sharing and Governance for Effective Cross-Agency and Industry Collaboration

Siva Karthik Devineni*, Rajath Karangara and Narayana Challa

Database Consultant, USA

ABSTRACT

Collaboration between public and private sectors is essential in today's complicated environment to tackle issues like financial crime and public health crises. Interoperability problems and complex data governance requirements are obstacles to safe data exchange, an essential part of this kind of cooperation. This study delves into the topic of safe data sharing methods that allow for collaboration between commercial companies (such pharma and fintech) and federal, state, and municipal governments. Data standardization and access control are among of the issues discussed, with examples from the pharmaceutical and financial technology industries to back up the claims of effective solutions. To overcome the data gap and harness the potential of industry and cross-agency cooperation for mutual benefit, this study argues for strong data governance frameworks and interoperable technology.

***Corresponding author**

Siva Karthik Devineni, Database Consultant, USA.

Received: September 11, 2023; **Accepted:** September 19, 2023; **Published:** September 29, 2023

Keywords: Data Security, Secure Data Sharing, Cross-Agency Collaboration, Interoperability, Data Governance, Pharma, Fintech, Trust, Innovation, Encryption, Access Controls, Authentication

Introduction

The need for secure data sharing mechanisms has become paramount as one passes through the era of increased cooperation between federal, state, and local agencies, and private industries. This paper discusses the difficulties and solutions associated with implementing these mechanisms, especially in sectors such as Pharma and Fintech. Its high-level intention is to provide a framework that fosters trust and ensures the confidentiality, integrity, and availability of shared data.

Secure data sharing is a way of transmitting or giving access to individual's personal information in a manner that secures the integrity, confidentiality, and availability. It helps prevent sensitive information from unauthorized access, breaches, theft, or accidental disclosure. Secure data sharing has several important features, such as encryption, access control and log auditing /monitoring [1]. Encryption muddles the data, keeping it unreadable to anyone without proper decryption key; access control limits who may read and write this information usually based on roles or permissions, while logging and monitoring record what's accessed by whom many even at specific time. Several security frameworks and regulations have been established to guide organizations in secure data sharing, including ISO/IEC 27001 and sector-specific regulations. Successful implementations of secure data sharing can be seen in case studies such as Cisco Systems, which uses a combination of robust data transfer protocols, advanced data encryption, and continuous education and training in data security to establish a secure data-sharing ecosystem [2].

Data sharing in cross agency collaboration can be a great tool for enhancing service delivery, solving complex problems, and ultimately creating benefits to citizens. Aggregating data from diverse agencies helps organisations recognize difficulties and find better solutions. For instance, it is crucial for pharmaceutical companies to share outcomes data with payers as their influence in treatment decision making increases. While payers and pharma have been sharing data for a while, data utilization is reaching new heights now and will continue to do so in the future [3].

Unmet social necessities including housing, food, and education put people and families at health risk [4]. Consequently, to meet these demands and increase coordination across health and social service sectors, attempts to enhance population health must go beyond the realms of medicine and public health [5]. One important part of these cross-sector partnerships that researchers have suggested for addressing inequalities and improving people's and communities' health and well-being is data exchange [6]. To comprehend and handle all their customers' social and health-related demands, several governments use integrated data systems (IDS) to connect administrative data at the person level across various human and health services [7].

Health care, public health, and social service systems may better address community health and well-being imbalances when they align across four basic enablers: common purpose, data, finance, and governance (the "Theory of Change"). Nevertheless, there are often obstacles to achieving this objective via cross-sector cooperation, with data exchange being cited as a major hurdle [8,9]. We looked at existing IDS (integrated data systems) to find out what the main obstacles and facilitators of data sharing are, so that cross-sector alignment initiatives may make better use of this information. One of the main goals of integrated data systems (IDS) is to connect data at the person level across different government programmes. This will help paint a full picture of how people's health, social service, and other needs are interrelated [10,11].

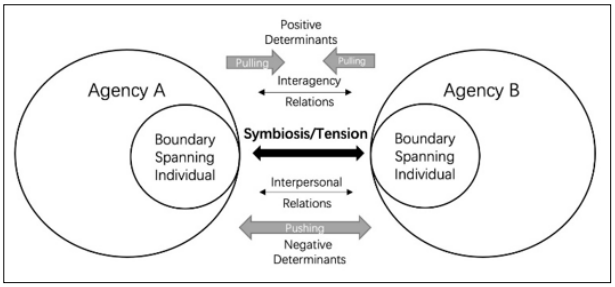

Figure 2: A Meta-Analysis of Interagency Government Data Exchange [12]

By offering several analytics tools pertaining to various domains, such as programme monitoring and evaluation, company operations, or case management information, IDS (integrated data systems) may enhance the decision-making capabilities of public administration and policymaking. As an example, integrated data systems (IDS) may be used in population-based longitudinal research to evaluate risk-protective variables, service utilization, case costs, and programme users' costs of care [11,13].

Collaborative Data Sharing: A Powerful Solution

In the modern world of interlocking jurisdictions, criminal activities often spill over across borders. It is no longer possible nowadays for neighbouring law enforcement agencies to function in isolation. By setting up procedures for sharing crime data, agencies will be able to access a larger reservoir of information. This collaborative approach enables the detection of patterns and trends that may otherwise have gone unnoticed on their own, therefore helping improve crime prevention-investigation processes. Four obvious advantages of data sharing are these:

Detecting Developing Crime Patterns

Through crime data sharing, law enforcement organisations can analyse it in many ways whereas they can identify new criminal patterns on a local basis. Agencies can monitor changes in criminal activity, identify problem areas and allocate resources where they are needed the most by integrating information from multiple jurisdictions. This comprehensive strategy may be more efficient and focused on the resultant law enforcement actions that would allow for a proactive fight against crime.

Strengthening Investigative Capacities

By transferring data between agencies, police may gain a clearer picture of what is currently going on with criminal behaviour. Through the sharing of data, different law enforcement organisations can further coordinate operations in improving efficiency and ensuring quick resolution of criminal cases. By this collaborative method of research, the success rate in investigations is improved as it unveils links between otherwise apparently irrelevant cases that allow criminals to function within several jurisdictions.

Improving Resource Allocation

Cross agency data sharing enables analysis of regional crime trends that provides law enforcement agencies with the ability to deploy their resources in an efficient manner. By identifying areas with a high crime rate, or even specific criminal activities that are on the rise, agencies can decide what personnel and assets they should have in those locations where they are needed the most. This tailored approach to applying law enforcement helps in pinpointing the areas where resources can be used best for raising public protection.

Proactive Crime Prevention

Another very powerful potential benefit of cross-agency data sharing is its ability to stem the tide before it happens, in other words proactive crime prevention. Establishing the latest crime patterns by law enforcement agencies can enable them to devise ultimate strategies and initiatives based on these tendencies before they become more severe. Sharing data on modus operandi, suspect descriptions and other relevant details allows effective interagency collaboration through the immediate execution of preventive countermeasures to thwart crimes or reduce their effect in the community.

Cross-agency collaborations are called as the one of solution for a reduction in inequities across different fields, such as healthcare, public health, and others; with effective data sharing involving all stakeholders would be crucial to deal with complex issues [5]. However, the efficient information exchange between partners can seem difficult for various reasons including protectiveness, mistrust, and uncertainty about whether sharing data with other agencies direct impacts on has reaching agency goals may be [14].

To overcome these challenges and facilitate successful data sharing, some key strategies and approaches include:

Establishing A Legal Framework for Appropriate Data Use

As a result of this, data is generated and shared in accordance with the legal provision concerning collection, storage sharing of individual or agency-based info [15].

Implementing Strong Data Governance

This involves obtaining commitment from the leadership of an agency, assessing capacities within each individual agencies and implementation of a data sharing agreement [14].

Advancing Data Literacy and the Role of Analytics in an Organization's Functions

This includes the right people to sit at the table. It means having good relationships and trust among all relevant stakeholders [5].

Developing Near Real-Time Insights

Because cross-agency data sharing is absolutely crucial for successful data analyses, agencies must sear out ways in which they can share their respective datasets that would be reflected within near real time and properly linked [16].

Ensuring Data Privacy and Security

As agencies aim to hasten data exchange, they focus on the concept of privacy and protection. Synthetic data can depict proceedings of certain populations without reflecting any specific person and as such help advance collaboration while ensuring protection of privacy [16].

Starting with a Small Group of Agencies

Initiatives usually start with a small set of agencies before expanding to include more data and users – both individuals and groups. This approach has helped to demonstrate the value gained from this initiative and earned trust among agencies [17].

Implementing Secure Data Sharing Mechanisms

Overview of Secure Data Sharing Protocols and Technologies

Data sharing is essential for cooperation in today's globally linked society. Modern collaborative initiatives rely on secure data exchange, which calls for strong standards and technology to protect sensitive information. Private information is in regular circulation between persons and organisations in all kinds of contexts, from

scientific studies to commercial endeavours. However, there is an element of danger associated with this interaction that must be properly covered to preserve confidentiality and integrity. Shared information needs to be protected with the help of security measures, such as identification, access restrictions and encryption to protect privacy integrity, authenticity.

Role of Encryption, Access Controls, and Authentication in Ensuring Data Security

A basic method is encryption, which converts plaintext to ciphertext that is incomprehensible to everyone except parties authorized with the right cryptographic keys. So, even though bad guys succeed at getting hold of the information they can't make anything out of it. Encryption forms the basis for safe data exchange, because as a digital vault it converts plaintext into an unintelligible cypher. Data can also be encrypted with secure methods, like AES and RSA when it's transferred or stored. The data becomes unreadable to anyone without the proper key. This ensures that data remains concealed even at the point of interception and forms the first line of protection [18].

Another measure to strengthen the security net is through access controls. Access controls serve as gatekeepers that help manage who can access and make changes to shared data. Fine-grained control can be driven by either context, data sensitivity or user roles. Using granular access control techniques like attribute-based access control, which regulates rights based on criteria like project team participation or security clearance and level, enables a far more precise approach [19]. These measures ensure that chances of abuse or unauthorized among are minimized and only authorized personnel with valid requirements can access the data.

Authentication is the last thread in the embroidery of effective data sharing techniques, and it is meant to confirm who people and devices seeking access to the data are. With multi-factor authentication (MFA) besides passwords, there is an additional security measure when verifying a user's identity because another factor must be confirmed. This can range from physical tokens to biometric verification. This minimizes the possibility of compromised credentials and attempts to impersonate other parties, which strengthens even more security of the data [20].

Case Studies Showcasing Successful Implementations in Collaborative Efforts

The fact that these protocols and technologies are successful is not only theoretical in nature – there are plenty of case studies which demonstrate their efficiency to use when the work is done collaboratively. The Human Genome Project was a monumental effort in international collaboration and implemented secure data sharing mechanisms to safeguard sensitive genetic information while allowing researchers across the globe contribute towards the project [21]. On a similar note, the CLOUD Act that is innovative agreement between US and EU made secure arrangement allowing law enforcement agencies in accessing data stored in cloud maintaining differential considerations of national security needs as well privacy concerns on data [22].

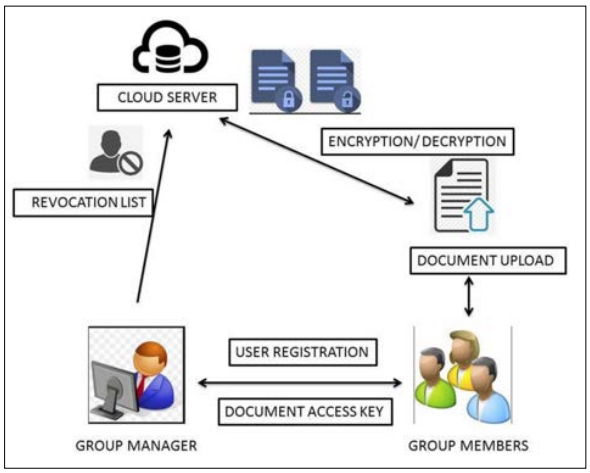

Figure 3: Secure Data Sharing in Cloud Environment [23]

Collaborative efforts and technologies have successfully implemented several secure data sharing protocols. One distinguishing characteristic is the application of blockchain technology. Decentralized and tamper-resistant blockchain technology protects shared data, making it perfect for trustworthy and open systems. For instance, in healthcare treatments, initiatives such as MedRec use a blockchain to enable secure sharing of patient data among the health care providers while maintaining the privacy and consent of patients.

SFTP is another common internet data encryption mechanism. It integrates the security functions of the SSH protocol with a secure file transfer operation to ensure that data can be safely exchanged between all parties involved. SFTP is used in various industries including the financial sector and law professionals to share sensitive information [24]. Federated identity management is needed for research collaborations. It enables sharing resources simple and secure for companies. Collaboration participants may access resources more securely and effectively utilizing federated identification protocols like SAML or OpenID Connect. Keeping different credentials for various systems is unnecessary.

Safe data exchange is the product of a sophisticated network of procedures including authentication, access control, and encryption, not just technology. With advanced methods and technology, businesses and people may connect online without worrying about personal information. As the globe becomes increasingly linked, information security will become more important. It will also try to improve itself in its quest for secure means to maintain our joint secrets.

Overcoming Challenges in Interoperability and Data Governance Research has demonstrated that data governance and interoperability are crucial for agencies and sectors to collaborate well. The best approach to define standards for data formats, protocols, and robust frameworks for the managing of data is by understanding the problems related to interoperability and data governance.

Analysis of Interoperability Challenges in Cross-Agency Collaboration

So in today's everchanging then world, the need for seamless coordination between the members of government is also very important. However, this route is often filled with challenges such as interoperability and data governance issues. Outside the silo, data is not always informative but can become a "great barrier" if agencies employ different formats and protocols, much less governance frameworks. In this essay, we discuss the complexities of these challenges and suggest actions that can be taken to achieve an integrated data environment that will ensure easy cross-agency collaboration.

Interoperability, which is the ability of distinct information management systems to share data and comprehend each other, poses a significant challenge.

A 2019 report by GAO shows agencies, including contributing human service organizations to the CIFR, are marred by inconsistencies in data formats used and compatibility of software systems or even varying security protocols. This fragmentation causes efforts duplication, delayed decision-making – hence slow provision of service delivery. Since disaster relief involves efforts by emergency responders and resource providers, the incompatibility among their databases presents a frightening result of gaps on interoperability.

Data standards are one of the foremost issues in interoperability and that there is simply a vast number of distinct information systems; typically, little to none can talk amongst themselves. This presents major technical and logistical problems which must be resolved for routine data sharing and integration to take place smoothly. To overcome these problems, data exchange standards and methodological and workforce model advantages must be established [25].

Strategies, employed to defeat interoperability challenges require the creation and deployment of common data standards and communication protocols. The use of widely accepted standards like XML, JSON or HL7 in healthcare can help agencies improve their interoperability by making the transmission and exchange of data known, easy to understand. Besides, the implementation of application programming interfaces (APIs) may serve as a middle ground between various systems whereby entering data does not necessitate an entire replacement of former infrastructure. These standards must also be a product of collaborative efforts by all stakeholders from different agencies so that the results can be as comprehensive, if possible, to accept.

Strategies for Establishing Standardized Formats and Protocols

To combat this fragmentation, standardized formats and protocols emerge as the saviour in shining armour. Standards like the FGDC (Federal Geographic Data Committee) and the NIEM (National Information Exchange Model) may help standardize communication [26]. Through the implementation of these standards across all agencies, it is ensured that data communicates in a common language, which in turn facilitates smooth interchange and cooperation.

Importance of Robust Data Governance Frameworks for Effective Collaboration

Another thing to consider as crucial is data governance, which guarantees that the data complies with standards of quality and security. Data governed cannot be easy when it comes to the number of stakeholders, regulations as well standards that need to be complied with. To create data governance, systems should have definite and constant roles, responsibilities, and regulations for data owners' customers, users' providers of details. Furthermore, data culture which consists of the perspectives and habits as well as mentality an organization has towards its work with data is much important to be discussed in terms on success of any implemented body or structure for declared governance [27].

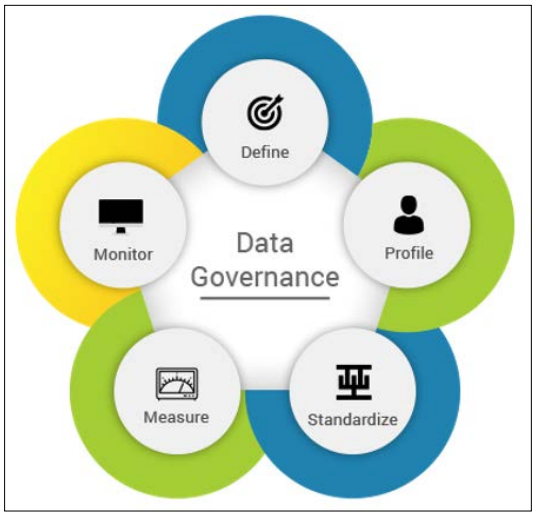

Figure 4: Data Governance - Gray Matter Analytics [28]

However, interoperability alone isn't enough. Sharing of data should also be robust at every stage to ensure the quality, security and ethical use is necessary through strong frameworks for governance on these matters [29]. This includes having defined ownership, access control and privacy policies. To further ensure that no errors or inconsistencies are introduced, solid frameworks include data quality monitoring and data lifecycle management. Envision the mayhem that would ensue if, at the height of a public health emergency, agencies disclosed inaccurate or out-of-date information because of poor leadership, putting the people's health and confidence at risk.

Establishing such frameworks can be possible only with not just technological solutions but also cultural changes. It is necessary to develop a culture of openness, trust, and data sharing between government bodies. This capability includes communication, cooperation, and training of developing officials with the right knowledge base to focus on finding its way through the data world. Efficient data governance frameworks are simply invaluable for successful cooperation between different government entities.

Defining effective data governance is "managing information at each point in its lifecycle, rules, processes and accountabilities". If trustworthy agencies that are involved in exchanging highly sensitive info rest assured that their data is securely protected by a well-arranged data governance system. It ensures that all parties conform to established norms and criteria, thus assisting participants in addressing issues related to data ownership, access, and integrity.

In the conclusion, since dealing with data governance and interoperability issues would be a multidimensional problem. Therefore, standardized formats and protocol might close the technology gap, and only strong data governance frameworks could ensure an ethical and responsible use of data. In the

end, though, what is most important is ensuring a culture of collaboration that treats data as community property for community interest. By breaking down data silos and establishing a single data environment, government departments may transition from operating as individual entities to becoming a well-orchestrated ensemble. Consequently, the agencies will have a platform through which they can collaborate to enhance service delivery for all stakeholders.

Comparative Pharma and Fintech Sectors

The inclination towards innovation in pharma-research and development (R&D), and the place it plays in financial technology known as Fintech, demands a protected space when data is to be collaborated. It might significantly speed up breakthroughs and simplify processes if sensitive information is shared, though it poses a serious security problem as well. If we analyse cases from both fields, we can identify the advantages and good practices to make this double-edged sword effective.

Case Study on Secure Data Sharing in Pharmaceutical Research and Development

Secure information sharing is a critical factor in the pharmaceutical field that helps to develop research issues. A significant project in this field is the partnership between drugmakers and research centres to speed up medicine finding. To overcome the obstacles of sharing secret information while preserving choices and security, mechanisms such as Observational Health Data Sciences and Informatics OHDSI have been introduced. OHDSI uses a standardized data-sharing infrastructure that enables researchers to aggregate and process health care information from various sources with safeguarding the anonymity of individuals while also fostering cooperation in science [30].

A study by PricewaterhouseCoopers PwC reveals that consumers are willing to share their health information with pharmaceutical companies, underlining the necessity of secure data collaboration [31]. Say, the case is with AstraZeneca and its partnership with University of Oxford for COVID -19 vaccine development. Furthermore, sharing of genomic data and clinical trial results in real-time turned out pivotal defining fast progress but at the same time raised doubts related to patient privacies and intellectual property [32]. To mitigate such concerns, the partners used an encrypted data sharing platform with fine-grained access control policies in place to ensure data integrity through minimizing unauthorized access [33]. This case illustrates the significance of finding a proper mix between collaboration and security characteristics – using effective data governance frameworks and technological solutions to enable secure transfer of data but control privacy and IP risks.

Also, a study in BMC Medicine points out the growing scope for sharing data materials during clinical trials stem from pharmaceutical companies; these people evidently have resource problems and need to resolve accessibility and management of databases [34].

Examination of Secure Data Collaboration within the Fintech Industry

Sharing information securely is of utmost importance in the Fintech business for the sake of keeping financial transactions honest and legitimate. Fintech companies must exchange financial and customer data in many instances to improve their services, but sensitive information calls for strong security measures. Analysis of secure data collaboration in the Fintech industry shows that users adopt blockchain technology to provide for transparency, security, and traceability in financial transactions. For instance, blockchain technologies have been used as a foundation for reliable and inalterable recording systems that would reduce the likelihood of fraud within the financial context [35].

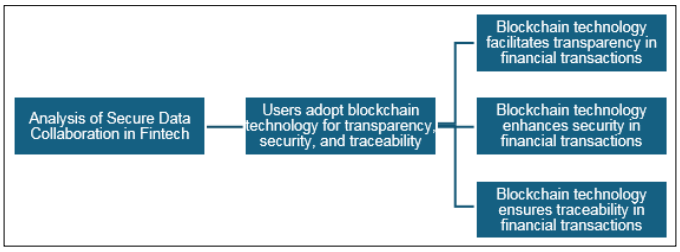

Figure 5: Analysis of secure data collaboration in the Fintech industry

For instance, Fintech companies have used data science to study banking databases, open financial data, customer information which contributed to better experiences in customer services and innovative initiatives built based on obtained data [36]. This further revolution in data has also taught some evident lessons to the bankers which indicate that there is an apparent requirement to devise and operate; innovate and implement the fintech data as driving force of transformation into a successful financial entity of this age.

Lessons Learned and Best Practices from These Sectors

Both pharmaceutical R&D and Fintech provide valuable insights for secure data collaboration. The first key observation is that effective data governance frameworks that dictate clearly defined roles, obligations, and access controls regarding sensitive information are critical [37]. Second, strong technology solutions should be invested in, such as secure platforms for sharing of data, encryption tools and methods to make data anonymous. Finally, the establishing of a culture within partnered collaboration that instils transparency and trust between collaborators is crucial to ensure they observe data security protocols right from the start for long term collaboration.

Lessons can be learned from these sectors and the best approaches identified. First, the creation of uniform structures such as those found in pharma with OHDSI enables secure data sharing by providing a level plain where collaboration can take place while still addressing privacy concerns. Moreover, making use of sophisticated technologies as such blockchain within the Fintech sector also implies that using state-of-the-art methods to maintain the confidentiality and inviolability of shared information is considered crucial. , regulatory compliance and meeting industry standards begin with limiting legal and ethical challenges of sharing information in both sectors [38].

Tools from these sectors teach the significance of engaging demand from customers, solving resource problems, and using data science to come up with secure and efficient ways by which information is shared. These perspectives can be used to formulate optimal guidelines for the secure sharing of data in pharmaceutical research and development, including consultancy services offered by fintech industries. By implementing these best practices, both the pharmaceutical and Fintech industries can benefit from such a collaboration of data at full capacity without impeding the risks in sharing sensitive information. By achieving the right mix of innovation and security, these industries can lay the foundation for a future based on data-driven progress while ensuring that

privacy and security exist among all interest groups.

To conclude, safe data sharing is one of the key elements of pharmaceutical research and Fintech's operation at the same time. Issues associated with privacy and security are illustrated by case studies in such fields, which show the importance of common structures as well as novel technologies that help to overcome such problems. if such large amounts of data are shared by these industries, dozens of lessons learned show the importance of behaviour as an organized group, conformity to state and industry regulations within it and underlines such trends as implementation leading edge technologies.

Conclusion

In solving difficult socioeconomic issues, cooperation among the various units is very important. Despite all this, there are interoperability and data governance issues that could stand in the way of sharing information between different government departments and commercial enterprises. This paper stated the importance of creating a legal framework for good data use, establishing effective data governance, enhancing data literacy, and acknowledging the analytics function in the operations of an organization. The research report also stated that many of the barriers in the way of cross-sector data sharing can be overcome by building trust with all parties involved and collaborating productively with them. This article presented examples from the pharmaceutical and financial technology industries, as well as practical measures that police departments should take to successfully establish cross-agency data sharing. When the report ends, it emphasizes the necessity of safe data sharing, which is becoming more important as collaborative efforts spread across both public and commercial sectors. The insights that were learned from the pharmaceutical and financial technology industries give essential lessons for learning how to create an environment that is both safe and sustainable for collaborative creation. When it comes to creating trust and ensuring effective cross-agency cooperation, the deployment of strong processes and the overcoming of interoperability difficulties are key measures that must be taken [39,40].

References

1. Secure Data Sharing and Compliance Frameworks (2023) Linkedin https://www.linkedin.com/pulse/secure-data-sharing-compliance-frameworks-lazarus-alliance.
2. What is Secure Data Sharing. SSH https://www.ssh.com/academy/secure-information-sharing/what-is-secure-data-sharing.
3. Taren Grom (2013) Commercialization Payers: The Power of Payer Partnerships Lies in Data Sharing. Pharma Voice https://www.pharmavoice.com/news/data-sharing/613479/.
4. Social Determinants of Health (2019) Centers for Disease Control and Prevention https://www.cdc.gov/about/sdoh/index.html.
5. Allen E, Samuel-Jakubos H, Waidmann T (2021) Data Sharing in Cross-Sector Collaborations Insights from Integrated Data Systems 1-2.
6. Landers GM, Minyard KJ, Lanford D, Heishman HA (2020) Theory of Change for Aligning Health Care, Public Health, and Social Services in the Time of COVID-19. Am J Public Health 110: S178-S180.
7. Network Sites. Actionable Intelligence for Social Policy https://aisp.upenn.edu/network-sites-map/.
8. Erickson J, Bobby Milstein, Lisa Schafer, Katy Evans Pritchard, Carly Levitz, et al. (2017) Progress Along the Pathway for Transforming Regional Health: A Pulse Check on Multi-Sector Partnerships. Rethink Health https://rethinkhealth.org/wp-content/uploads/2017/03/2016-Pulse-Check-Narrative-Final.pdf.
9. Spillman BC, Leopold J, Allen EH, Blumenthal P (2017) Developing Housing and Health Collaborations: Opportunities and Challenges. Urban Institute https://www.urban.org/sites/default/files/publication/89581/2001225_developing_housing_and_health_collaborations.pdf.
10. Integrated Data Systems Map. Actionable Intelligence for Social Policy https://aisp.upenn.edu/integrated-data-systems-map/.
11. Byrne T, Metraux S, Moreno M, Culhane D P, Toros H, et al. (2012) Los Angeles County's Enterprise Linkages Project: An Example of the Use of Integrated Data Systems in Making Data-Driven Policy and Program Decisions. California Journal of Politics and Policy 4: 95-112.
12. Zhou L, Hu J, Xu J (2022) Understanding interagency relationships in the sharing of government data: a meta-analysis. Information Research: an international electronic journal 27.
13. Cutuli JJ, Robert M Goerge, Claudia Coulton, Maryanne Schretzman, David Crampton, et al. (2016) From foster care to juvenile justice: Exploring characteristics of youth in three cities. ASIP 67: 84-94.
14. Coordinating data sharing across agencies, Strategies to Address Common Challenges (2021) HSRA https://mchb.hrsa.gov/sites/default/files/mchb/programs-impact/coordinating-across-agencies.
15. Cross-Agency Data Sharing Promises Benefits for All (2022) GovTech https://www.govtech.com/opinion/cross-agency-data-sharing-promises-benefits-for-all.
16. Sarah Sybert (2022) Data-Sharing Initiatives Are Helping Agency Decision-Making. Govcio https://govciomedia.com/data-sharing-initiatives-are-helping-agency-decision-making/.
17. Yaroni A, Ross T (2014) Innovations in NYC Health and Human Services Policy Data Integration and Cross-Agency Collaboration 1: 5-6.
18. Stallings W (2017) Cryptography and network security: principles and practice Boston: Pearson Prentice Hall https://www.cs.vsb.cz/ochodkova/courses/kpb/cryptography-and-network-security_-principles-and-practice-7th-global-edition.pdf.
19. Sushmita Ruj (2014) Attribute based access control in clouds: A survey. IEEE Explore https://ieeexplore.ieee.org/document/6983992.
20. Duo Trusted Access, Duo Security. Cisco Duo https://duo.com/.
21. National Human Genome Research Institute (2020) The Human Genome Project https://www.genome.gov/human-genome-project.
22. Cloud computing. Shaping Europe's digital future https://digital-strategy.ec.europa.eu/en/policies/cloud-computing.
23. Sita Kumari Kotha, Meesala Shobha Rani, Bharat Subedi, Anilkumar Chunduru, Aravind Karrothu, et al. (2021) A Comprehensive Review on Secure Data Sharing in Cloud Environment. Wireless Personal Communications 127: 2161-2188.
24. Ssh.com (2013) SFTP File Transfer Protocol. Get SFTP client & server | SSH.COM https://www.ssh.com/ssh/sftp/.
25. Martin LT, Christopher Nelson, Douglas Yeung, Joie D. Acosta, Nabeel Qureshi, et al. (2022) The Issues of Interoperability and Data Connectedness for Public Health.

10: S19-S24.

26. National Information Exchange Mode. NIST https://www.nist.gov/document/ansi-nistarchivedxmlday3yuh.
27. What are the challenges of interoperability in digital manufacturing? Linked in https://www.linkedin.com/advice/0/what-challenges-interoperability-digital-wakwc.
28. Fuller S (2019) The First Step Towards Interoperability Is Data Governance. Gray Matter Analytics https://www.graymatteranalytics.com/2019/05/the-first-step-towards-interoperability-is-data-governance/.
29. Steer D (2021) Council Post: Best Practices in Data Governance Forbes. Forbes https://www.forbes.com/sites/forbestechcouncil/2021/09/08/best-practices-in-data-governance/.
30. Hripcsak G, Jon D Duke, Nigam H Shah, Christian G Reich, Vojtech Huser, et al. (2015) Observational Health Data Sciences and Informatics (OHDSI): Opportunities for Observational Researchers. Studies in Health Technology and Informatics 216: 574-578.
31. Opportunities for FinTech in the Pharmaceutical Industry (2022) Prove https://www.prove.com/blog/opportunities-for-fintech-in-pharmaceutical-industry.
32. Corum J, Zimmer C (2020) How the Oxford-AstraZeneca Vaccine Works. The New York Times https://www.nytimes.com/interactive/2020/health/oxford-astrazeneca-covid-19-vaccine.html.
33. How fast can vaccination against covid-19 make a difference. (2021) The Economist https://www.economist.com/science-and-technology/2021/01/23/how-fast-can-vaccination-against-covid-19-make-a-difference.
34. Hopkins AM, Rowland A, Sorich MJ (2018) Data sharing from pharmaceutical industry sponsored clinical studies: audit of data availability. BMC Medicine 16: 1-6.
35. Mougayar W (2016) The Business blockchain: promise, practice, and application of the next internet technology. Hoboken: John Wiley & Sons https://www.wiley.com/en-in/+Business+Blockchain%3A+Promise%2C+Practice%2C+and+Application+of+the+Next+Internet+Technology-p-9781119300311.
36. Data Science in Fintech Industry: Examples and Use Cases. (2022) HQSoftware https://hqsoftwarelab.com/blog/data-science-in-fintech-industry-examples-and-use-cases/.
37. Practical guide GDPR data protection officers. CNIL https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-gdpr_practical_guide_data-protection-officers.
38. Mitchell H, Amie J Eisfeld, Amy C Sims, Jason E McDermott, Melissa M Matzke, et al. (2013) A Network Integration Approach to Predict Conserved Regulators Related to Pathogenicity of Influenza and SARS-CoV Respiratory Viruses. PLOS ONE 8: e69374-e69374.
39. Forum WE (2021) From competition to collaboration: How secure data sharing can enable innovation. European Sting https://europeansting.com/2021/06/28/from-competition-to-collaboration-how-secure-data-sharing-can-enable-innovation/.
40. Cross-Agency Collaboration: Information Sharing For Combined Success (2020) Tesla Government https://teslagov.com/cross-agency-collaboration-information-sharing-for-combined-success/.