

---

## Addressing Database Interoperability Challenges to Enhance Organisational Collaboration



---

Effective data sharing among collaborating organisations is highly desirable but often challenging due to varying database management systems (DBMSs), different data schemas, and protection policies. Trust in the data-sharing system is paramount, particularly when allowing external queries into internal databases. Current industry solutions are fragmented and fail to comprehensively and securely achieve all data-sharing objectives. A study published in JAMIA Open aimed to tackle database interoperability challenges that hinder effective collaboration among different organisations. The authors aimed to improve data sharing while ensuring that local data protection policies remain intact. They developed a novel solution designed to overcome these challenges. It requires no changes to existing DBMSs or authentication methods, making it seamless to integrate into current operations.

### Innovative SFDS: Leveraging NDAC and DBM for Secure, Granular Data Sharing

Researchers developed a lightweight system called the Secure Federated Data Sharing System (SFDS) to facilitate broad yet well-regulated data sharing. This system was constructed using two advanced technologies developed by the National Institute of Standards and Technology (NIST): Next-generation Database Access Control (NDAC) and the Data Block Matrix (DBM).

NDAC is a sophisticated access control mechanism that regulates access to database resources at a granular level, based on user attributes. This means that access can be controlled down to individual fields in a database, ensuring that users can only access data that they are authorised to see.

DBM is responsible for managing and sharing user attribute assignments across a network of organisations. This is implemented using a modified open-source permissioned blockchain, ensuring that user attributes are authoritative and securely shared among the participating entities.

A proof-of-concept system was created using synthetic data, simulating a clinical research data-sharing scenario to validate the approach. This allowed us to demonstrate how the SFDS could be used in real-world applications.

### Effective Integration and Secure Data Sharing with SFDS: A Clinical Research Use Case

Through a consent-based model, authors successfully demonstrated how previously unknown users could be integrated into NDAC by assigning them DBM-validated attributes. This enabled these users to access local database resources in accordance with established policies. The key components of SFDS—NDAC and DBM—performed exceptionally well, showcasing strong performance metrics. The system's ability to provide detailed, attribute-based access control was particularly noteworthy.

The SFDS ensures secure data sharing by validating mandatory user attributes and assigning discretionary attributes to control access to local data. This system effectively enables sharing of data, such as patient condition details, with external research organisations without exposing sensitive information or compromising data integrity. By using a clinical research use case, we demonstrated how the SFDS facilitates secure data sharing among disparate organisations while maintaining local data protection policies. This system allows data to remain within its home organisation, avoiding the risks associated with data exchange or central storage.

### SFDS: Advancing Data-Sharing Infrastructure with Transparency and Security

The SFDS represents a significant advancement in data-sharing infrastructure. It offers a secure and effective method for achieving data-sharing

goals without disrupting the normal business operations of participating organisations. One of the major advantages of SFDS is its transparency; it requires no modifications to existing database management systems or to the methods used for authenticating and authorising local users. Moreover, the SFDS's ability to authenticate external users through DBM-validated attributes and then assign them discretionary attributes for local data access addresses a crucial need in data-sharing practices. This approach ensures that data protection policies are upheld while facilitating seamless collaboration.

The SFDS is an efficient, flexible, and granular solution that meets the data-sharing and protection needs of the clinical research community. Its practical deployment and control capabilities make it an ideal choice for organisations looking to share data securely without compromising local policies.

**Source:** [JAMIA Open](#)

**Image Credit:** [iStock](#)

Published on : Tue, 21 May 2024