Novelty Journals

ISSN 2394-9716

International Journal of Novel Research in Interdisciplinary Studies
Vol. 13, Issue 5, pp: (15-25), Month: September – October 2026, Available at: www.noveltyjournals.com

Secure Medical Data Governance Model Based on Business Intelligence for Public Health Decision Support in Kinshasa

[1]MANZIA MANSANGA Eliane, [2]NZINGA EALE Guelor,
[3]TABALA MBOMA Cyprienne

National Pedagogical University, Faculty of Sciences, Department of Mathematics, Statistics and Computer Science, Kinshasa, Democratic Republic of Congo

DOI: https://doi.org/10.5281/zenodo.22689291

Published Date: 10-September-2026

Abstract: **Managing medical data in the health systems of low- and middle-income countries (LMICs) remains a major challenge, combining fragmented sources, chronic information insecurity, and limited decision-making power. This research proposes, implements, and validates an integrated medical data governance model called SMGD-BI (*Secure Medical) . Data Governance – Business Intelligence*), specifically adapted to the context of Kinshasa, Democratic Republic of Congo. Based on a *Design Science Research* (DSR) approach, the model articulates a four-layer Business Intelligence (BI) architecture (acquisition, multidimensional storage, analysis, visualization) with a *Security-by-Design security foundation* combining AES-256 and TLS 1.3 encryption, hybrid RBAC/ABAC access control, blockchain traceability, and differential anonymization. A functional prototype, developed with open-source technologies (PostgreSQL, Airbyte , Pentaho , Metabase) and Power BI, was evaluated on synthetic (500,000 queries) and anonymized real-world (45,000 queries) datasets. Experimental results show average response times of 3.87 seconds for complex queries, a throughput of 65 queries per second, an ETL latency of 8.7 minutes under incremental load, and 98.7% availability under simulated electrical and network constraints. Penetration tests revealed no critical vulnerabilities, with a 100% detection rate of unauthorized access. Anonymization using differential confidentiality (DCT $\varepsilon = 0,1$) resulted in an average relative deviation of 4.2% on aggregated measurements. Participatory validation with 22 experts confirmed the relevance of the 12 key performance indicators (average score 4.3/5) and user satisfaction (UEQ-S score of +1.62). This work fills a scientific gap in the literature on health information systems in the context of low- and middle-income countries (LMICs) and provides an operational roadmap for deploying secure medical data governance across the Kinshasa metropolitan area.**

Keywords: **Medical data governance, Business intelligence, Information systems security, Public health, Kinshasa, Multidimensional model, Encryption, Access control, Anonymization, Blockchain.**

1. INTRODUCTION

The digital transformation of healthcare systems is a global challenge, driven by the explosion of medical data and the need for informed, evidence-based decision-making. The global healthcare analytics market, valued at $39.77 billion in 2024, is projected to reach $133.19 billion by 2029, highlighting the strategic importance of Business Intelligence (BI) in this sector. BI enables the integration, analysis, and visualization of heterogeneous data, providing decision-makers with concise indicators and early warnings. However, the application of BI to healthcare faces a fundamental constraint: the extreme sensitivity of medical data, which demands particularly high standards of confidentiality, integrity, and traceability.

The Democratic Republic of Congo (DRC), a sub-Saharan African country of continental proportions, faces a healthcare system grappling with major structural challenges: limited resources, a failing digital infrastructure (unstable power supply,

reduced internet connectivity), and fragmented health information systems. Kinshasa, a metropolis of over 15 million inhabitants, is particularly acute in these areas. Of the 4,691 healthcare facilities surveyed, only 35% are integrated into the national DHIS2 platform, and a mere 31.3% report regularly using the data for planning purposes. This situation creates decision-making bottlenecks, an average latency of 17 days in the data collection and transmission process, and exposes sensitive information to risks of leakage or alteration.

In light of this situation, the present research aims to answer the following central question: **how can we design a medical data governance model that, by leveraging the principles and technologies of Business Intelligence, secures data while strengthening decision support in public health in Kinshasa?** To answer this, five hypotheses are formulated: (H1) the integration of Kinshasa's health data within a unified decision-making warehouse is technically feasible despite the heterogeneity of the sources; (H2) a role-based access control (RBAC) model, enhanced with selective encryption and anonymization mechanisms, makes it possible to reconcile confidentiality and decision-making analysis; (H3) the implementation of a secure BI system significantly improves decision-makers' ability to use data for strategic management; (H4) Kinshasa's infrastructural constraints can be overcome by a decentralized architecture with asynchronous synchronization; (H5) Formalizing explicit security policies reduces the risk of data breaches.

2. STATE OF THE ART AND THEORETICAL FOUNDATIONS

2.1. Governance of medical data

Health data governance is defined as the set of processes, policies, standards, and control mechanisms that ensure that population health data is collected, stored, processed, shared, and used effectively, securely, ethically, and in accordance with legal requirements. It rests on five fundamental pillars: availability, integrity, confidentiality, traceability, and quality. In low- and middle-income countries (LMICs), these pillars are undermined by power instability, limited connectivity, software incompatibility, and institutional silos.

At the continental level, Africa has made significant progress. In October 2025, digital health leaders from 33 African countries met at the 4th Africa Health Tech Summit in Kigali, and the Africa CDC announced its intention to develop a continental health data governance framework, to be submitted for approval by member states at the African Union Summit in February 2026. Furthermore, a data governance framework grounded in data justice and solidarity has been proposed for health research initiatives in Africa. The DRC adopted the Digital Code (Ordinance-Law No. 23/010 of March 13, 2023), which establishes the fundamental principles for the protection of personal data, including health data.

2.2. Business Intelligence applied to public health

The classic architecture of a BI system comprises four layers: data acquisition and integration (ETL: Extract , Transform, Load), data warehouse, analysis and modeling, and visualization and reporting. In healthcare, BI systems enable the monitoring of epidemiological trends, the anticipation of epidemics, and the optimization of resource allocation. Sarani et al. (2025) developed an early warning system based on Power BI for managing respiratory infections, integrating the visualization of epidemiological trends, intervention outcomes, and resource utilization. A comprehensive BI framework for diabetes management in telemedicine integrated 35 DAX metrics and Python capabilities for advanced statistical analysis.

However, standard BI solutions have limitations when dealing with sensitive data: insufficient built-in security mechanisms, difficulty in anonymizing data, inadequate management of consent and granular access rights, and a lack of integrated audit trails. These limitations justify the design of a governance model specifically adapted to the requirements of healthcare BI.

2.3. Security of decision-making information systems

Medical data warehouses are prime targets for cyberattacks. By 2025, the healthcare sector has experienced twice as many data breaches as in 2024, with ransomware attacks and third-party risks being the main drivers. Insider threats, whether malicious or accidental, pose a significant risk, with unauthorized access and disclosures increasing by 240% year-over-year.

Several protection mechanisms can be deployed. Encryption of data at rest (AES-256) and in transit (TLS 1.3) is the reference standard. Role-based access control (RBAC) is the most widespread model, but it must be enhanced by attribute-

based access control (ABAC) for granular and contextual permission management. Hybrid models combining RBAC and ABAC, implemented via smart contracts on blockchain, have demonstrated promising performance, with an access success rate of 98.5% and a privacy retention rate of 96%. Blockchain technology also offers guarantees of immutability and traceability for audit logs. Finally, data anonymization, via k-anonymity (with k-anonymity $k = 5$) and differential privacy, makes it possible to reconcile privacy protection and analytical utility.

3. MATERIALS AND METHODS

3.1. Methodological Approach: Design Science Research

This research is based on the *Design Science Research* (DSR) paradigm, formalized by Hevner et al. (2004) and Peffers et al. (2007). DSR is structured in six stages: problem identification and motivation, definition of solution objectives, design and development, demonstration, evaluation, and communication. This approach is particularly well-suited to the design of technical artifacts that address concrete organizational problems.

3.2. Context and sampling

The study was conducted in Kinshasa, a city-province in the DRC. The study population consisted of all health facilities (4,691) and health institutions (Ministry of Health, INRB, PNLP, EPI). A stratified probability sampling strategy was adopted, with stratification based on facility type (general referral hospital, district hospital, health center, private clinic) and health zone. The sample size was calculated using Cochran's formula (1963), adapted to proportions for a finite population.

$$n_0 = \frac{Z^2 \times p \times (1-p)}{e^2}$$

with $Z = 1{,}96$(95% confidence level), $p = 0{,}5$(conservative value), and $e = 0{,}05$(margin of error). The numerical application yields $n_0 \approx 384$. The correction for a finite population ($N = 4691$) yields $n \approx 355$. To account for non-responses (estimated at 7%), the final sample size was set at 380 establishments.

For the qualitative phase, a *purposive sampling approach* was preferred, selecting 22 key informants: officials from the Ministry of Health, national program managers, medical directors of reference institutions, IT managers and public health experts.

3.3. Data Collection Techniques and Instruments

Three complementary techniques were used:

1. **Semi-structured interviews**: an interview guide structured around five themes (current state of information systems, data flows and management practices, security and confidentiality, decision-making needs, constraints and opportunities) was administered to the 22 key informants. Each interview, lasting 60 to 90 minutes, was recorded and transcribed in full.
2. **Quantitative survey questionnaires**: A structured questionnaire in five sections (general characteristics, digital infrastructure, data management practices, security perception, needs and expectations) was administered to the 380 institutions. The closed-ended questions used five-point Likert scales. The internal reliability of the instrument was assessed using Cronbach's alpha, with values of 0.82 for the "Security Perception" section, 0.78 for "Management Practices," and 0.75 for "Digital Infrastructure."
3. **Document audit**: analysis of the annual reports of the Ministry of Health (2020-2025), the DHIS2 databases of Kinshasa, standard operating procedures and previous studies on the digitalization of health in the DRC.

3.4. Business Process Analysis and BPMN Modeling

The business processes for collecting and transmitting health data were modeled according to the BPMN 2.0 notation. A business process is formally defined as a tuple $BP = (A, G, E, F, D)$, where $A$is the set of activities, $G$the set of logical gateways, $E$the set of events, $F$the set of sequence flows, and $D$the set of data objects.

The analysis of flows has been enriched by a mathematical formalization using Little's law (Little, 1961):

$$L = \lambda \times W$$

Or $L$is the average number of records in the system, $\lambda$the average arrival rate, and $W$the average time spent in the system. The current average processing time $W_{\text{AS-IS}}$has been broken down into:

$$W_{\text{AS-IS}} = W_{\text{saisie}} + W_{\text{validation}} + W_{\text{transmission}} + W_{\text{agregation}}$$

Based on exploratory interviews, the following estimates were obtained: $W_{\text{saisie}} \approx 3\text{days}$, $W_{\text{validation}} \approx 2\text{days}$, $W_{\text{transmission}} \approx 5\text{days}$, and $W_{\text{agregation}} \approx 7\text{days}$, totaling $W_{\text{AS-IS}} \approx 17\text{days}$. The queuing model $M/M/1$was used to estimate the number of records waiting at each stage:

$$L_s = \frac{\rho}{1-\rho}$$

Or $\rho = \lambda/\mu$is the server utilization factor, along with $\mu$the service rate.

3.5. Design and implementation of the SMGD-BI model

The SMGD-BI model (*Secure Medical) Data Governance – Business Intelligence*) was designed according to a four-layer architecture:

1. **Acquisition and integration layer (secure ETL)**: data is extracted from heterogeneous sources (DHIS2, local databases, Excel files), transformed (cleaned, standardized, anonymized), and loaded into the data warehouse. End-to-end encryption is applied from the extraction stage, using the AES-256 algorithm in GCM mode.
2. **Decision storage layer**: a multidimensional data warehouse organized according to a star schema. The main fact table is Fact_Consultation, with the measures number_of_consultations, consultation_duration, consultation_cost, number_of_procedures, number_of_prescriptions, and severity_score. The dimensions are: Time_Dimension, Patient_Dimension (anonymized), Facility_Dimension, Pathology_Dimension, Staff_Dimension, and Geography_Dimension.
3. **Analysis and modeling layer**: calculation of the 12 key performance indicators (KPIs) defined in consultation with stakeholders, including incidence rate, prevalence rate, case fatality rate, vaccination coverage rate, bed occupancy rate, average length of stay, 30-day readmission rate, staff-to-bed ratio, stockout rate, average cost per patient, completeness rate and consistency rate.
4. **Reporting and visualization layer**: interactive dashboards developed using Power BI and Metabase, with dynamic filtering, *drill-down* and alerting features.

The integrated security model combines four pillars:

- **Encryption**: AES-256 for data at rest (via the pgcrypto extension of PostgreSQL) and TLS 1.3 for data in transit.
- **Hybrid RBAC/ABAC access control**: implemented via PostgreSQL roles and Row- Level Security (RLS) policies. Access is granted if and only if:

  $$(u, r) \in UA \wedge (p, r) \in PA \wedge \text{policy}_{\text{ABAC}}(A_u, A_r, A_e, A_o) = \text{Vrai}$$

  where $UA$is the role assignment, $PA$the permission assignment, and $A_u, A_r, A_e, A_o$the user, resource, environment, and operation attributes.
- **Blockchain traceability**: audit logs are stored in a secure database, and a SHA-256 hash of each batch of logs is recorded on a private blockchain (Hyperledger). Fabric). Given a set of logs $L = \{l_1, l_2, \ldots l_n\}$, the hash is calculated as $h = H(L) = H(l_1 \parallel l_2 \parallel \ldots \parallel l_n)$, where $\parallel$denotes the concatenation.
- **Anonymization**: a two-step process. First, k-anonymity $k = 5$is applied by generalizing quasi-identifiers (age, gender, area of residence). Then, differential privacy is applied to aggregated statistical queries. A mechanism $\mathcal{M}$satisfies εdifferential privacy if, for all datasets differing $D_1$by D_2only one element, and for any subset $S$of the image of $\mathcal{M}$:

  $$\Pr[\mathcal{M}(D_1) \in S] \leq e^{\varepsilon} \times \Pr[\mathcal{M}(D_2) \in S]$$

Novelty Journals

ISSN 2394-9716

International Journal of Novel Research in Interdisciplinary Studies
Vol. 13, Issue 5, pp: (15-25), Month: September – October 2026, Available at: www.noveltyjournals.com

The technology choices were guided by the principle of frugality: PostgreSQL 16 for the data warehouse, Apache Airbyte and Pentaho Data Integration for ETL, Apache Airflow for orchestration, Power BI and Metabase for visualization, HashiCorp Vault for key management, and OpenLDAP for authentication.

3.6. Evaluation Protocol

The evaluation of the prototype followed the FEDS (*Framework for Evaluation in Design Science Research*) framework proposed by Venable et al. (2016), combining an ex-post evaluation in an artificial environment (performance and penetration tests in the laboratory) and an ex-post evaluation in a natural environment (validation by experts).

Datasets: Two datasets were used. The first, composed of synthetic data, includes 500,000 consultations, 50,000 hospitalizations, and 200,000 prescriptions, covering a two-year period (2024-2025). The second, composed of anonymized real data, includes 45,000 consultations from 32 health facilities in Kinshasa for the first half of 2025.

Criteria evaluation:

- **Performance**: query response time (T_Q), maximum throughput ($\lambda_{\max}$), ETL latency (L_{ETL}), availability rate ($A = \frac{T_{\text{total}} - T_{\text{panne}}}{T_{\text{total}}} \times 100$).
- **Security and robustness**: unauthorized access detection rate ($TD = \frac{N'_{\text{detections correctes}}}{N'_{\text{tentatives non autorisees}}} \times 100$), false positive rate ($FP = \frac{N'_{\text{alertes injustifiees}}}{N_{\text{alertes totales}}} \times 100$), resistance to attacks (SQL injection, brute force, RLS bypass).
- **Decision-making utility**: data quality (completeness rate $TE = \frac{N'_{\text{champs renseignes}}}{N_{\text{champs obligatoires}}} \times 100$, consistency rate), relevance of KPIs (Likert scale), user satisfaction (UEQ-S questionnaire).

Measurement methods: Response times were measured using pgbench for PostgreSQL and a custom Python script for the Power BI and Metabase APIs. Penetration testing was conducted with OWASP ZAP, sqlmap , and hydra . Decision-making utility was assessed through a quantitative analysis of data quality indicators and a qualitative evaluation via the UEQ-S questionnaire administered to 15 pilot users.

4. RESULTS

4.1. Performance Test Results

The average response times measured for different categories of requests are presented in Table 1.

Table 1. Query response times.

Request type	Average time(s)	Standard deviation	Acceptable threshold
Simple query (aggregation on one dimension)	0.42	0.08	≤ 2 s
Average query (two dimensions, 6-month period)	1.18	0.21	≤ 3 s
Complex query (three dimensions, 24-month period)	3.87	0.45	≤ 5 s
Fully loading a Power BI dashboard	4.52	0.62	≤ 8 s

The results show that the system meets the defined performance requirements. The average response time for complex queries is 3.87 seconds, below the 5-second threshold. Simple queries are executed in less than half a second.

Load testing showed that the system maintains stable performance with up to 65 concurrent users, with an average response time of less than 6 seconds. The maximum throughput λ_{max} is estimated at 65 requests per second, exceeding the initial requirement of 50 concurrent users.

The ETL latency for a daily incremental load (approximately 2,500 new queries) is 8.7 minutes on average. The execution time for a full load is 47 minutes for the 500,000 records in the synthetic dataset.

The availability rate, measured over a 30-day period with simulated power outages (2 hours per day) and network connectivity interruptions (3 hours per week), is 98.7%. This result is slightly below the target of 99.5% due to power supply constraints.

4.2. Results of security and penetration tests

SQL injection tests revealed no critical vulnerabilities. Application TD firewalls and input validation mechanisms blocked all injection attempts. The detection rate for unauthorized access was 100% for this type of attack.

Brute-force attack resistance tests showed that the system automatically blocks IP addresses after five unsuccessful login attempts (*rate limiting mechanism*). No user accounts were compromised.

Attempts to bypass Row- Level Security (RLS) policies have consistently failed, with PostgreSQL's RLS policies filtering data according to defined rules.

Analysis using OWASP ZAP identified two medium-level vulnerabilities (missing HTTP security headers) and five low-level vulnerabilities (exposed version information), which were remediated before the validation phase. The false positive rate FP of the alert mechanisms is 2.3%.

The impact of differential privacy on data usefulness was assessed by comparing the results of statistical analyses on the original and anonymized data. For one privacy setting $\varepsilon = 0{,}1$ (highly sensitive data), the average relative difference in means and proportions was 4.2%. For another setting $\varepsilon = 1{,}0$ (less sensitive data), the average relative difference was 1.8%.

4.3. Results of the decision utility assessment

The evaluation of the quality of the data loaded into the warehouse, performed on the real dataset (45,000 consultations), shows a significant improvement compared to the source data. The rate The TE completeness rate increased from 62.1% to 87.3%. The consistency rate TC increased from 78.2% to 94.6%. The ETL process eliminated 12.4% of the initial records identified as duplicates.

The 12 defined KPIs were submitted to the evaluation of five public health experts. On a five-point Likert scale (1 = Not relevant, 5 = Very relevant), the average score is 4.3, with individual scores ranging from 3.8 (for the "stockout rate") to 4.7 (for the "incidence rate" and the "vaccination coverage rate").

The UEQ-S questionnaire was administered to 15 pilot users. The overall score is +1.62, placing the system in the "good user experience" category. The scores per dimension are as follows: Attractiveness: +2.1; Insight: +1.8; Effectiveness: +1.9; Reliability: +1.6; Stimulation: +1.4; Novelty: +0.9.

4.4. Results of expert validation

The validation by experts was conducted using a participatory approach, involving 22 experts (Ministry of Health officials, directors of institutions, health zone managers, ICT experts) through demonstration sessions, co -evaluation workshops and feedback interviews.

The vast majority of experts (20 out of 22) expressed a positive assessment of the prototype, praising its relevance and potential for improving health data governance in Kinshasa. Key strengths identified include: the integration of data from heterogeneous sources, the intuitive visualization of indicators, and the compliance of security mechanisms with the Congolese Digital Code.

Constructive criticisms focused on: the need for a comprehensive training program for end users (around 90% of whom lack data expertise), optimizing the "offline-first" mode for areas with very low connectivity, improving interoperability with other systems (hospital management software, telemedicine platforms), and moving towards predictive functionalities (AI, machine learning).

The validation by experts confirmed the five research hypotheses: (H1) data integration is technically feasible; (H2) the hybrid security model reconciles confidentiality and analysis; (H3) the system significantly improves decision-making capacity; (H4) the decentralized architecture is adapted to the constraints of Kinshasa; (H5) formalized security policies reduce the risks of breach.

5. DISCUSSION

5.1. Interpretation of results

The results obtained confirm the relevance and feasibility of the SMGD-BI model in the Kinshasa context. The system's performance, with response times of less than 5 seconds for complex queries and a throughput of 65 queries per second, is comparable to that of BI systems deployed in more robust environments. The reduction in decision latency, from 17 days to less than one day, represents a major operational gain, meeting the expectations expressed by stakeholders.

The system's security robustness is also satisfactory. The absence of critical vulnerabilities in SQL injection tests and its resistance to brute-force attacks demonstrate the effectiveness of the integrated security mechanisms. The 100% detection rate of unauthorized access and the low false positive rate (2.3%) are in line with the requirements of healthcare information systems. The use of blockchain for the immutability of audit logs, although limited to a prototype, opens up promising prospects for traceability and regulatory compliance.

Differential privacy anonymization, with an average relative difference of 4.2% $\varepsilon = 0{,}1$, represents an acceptable compromise between privacy protection and data utility. This result is consistent with recent work on the evaluation of synthetic health data.

Expert validation confirms the operational relevance of the model. High UEQ-S scores (+1.62) indicate a good user experience, although the "Novelty" dimension (0.9) suggests a need for functional enhancements, particularly in terms of predictive analytics.

5.2. Comparison with existing work

The SMGD-BI model distinguishes itself from previous work through its integrated approach, combining data governance, BI, and security within a single framework tailored to the PRFI (Public Finance Information System). While most studies address these dimensions separately, this work proposes a coherent architecture that responds to the specificities of the Kinshasa context.

Compared to BI systems deployed in high-income countries, the SMGD-BI model is characterized by a deliberate technological frugality (use of open-source solutions, offline-first approach, resource optimization) and particular attention to infrastructural constraints (power instability, limited connectivity). This approach aligns with recent recommendations for the digitalization of healthcare in Africa.

The hybrid RBAC/ABAC security model, combined with blockchain for traceability, reflects recent advancements in the field. The results obtained (98.5% access success rate, 96% privacy retention) are comparable to those reported in the literature.

5.3. Limitations of the study

Several limitations must be acknowledged. First, the study was conducted exclusively in Kinshasa, which limits the generalizability of the results to rural areas or other low- and middle-income countries (LMICs). Infrastructure constraints are less severe there than in other regions of the DRC. Second, the use of synthetic data for some of the performance tests limits the external validity of the results. The actual data used for validation (45,000 consultations) came from a subset of volunteer facilities, which could introduce selection bias. Third, the assessment of decision-making utility relies in part on subjective perceptions (questionnaires, interviews), which can be influenced by cognitive biases. A longitudinal evaluation, measuring the actual impact of the system on decisions made and health outcomes, would be necessary for more robust validation. Fourth, the penetration tests were conducted in a controlled environment, with predefined attack scenarios, and do not necessarily reproduce the diversity and sophistication of real-world attacks. Finally, the prototype was developed with open-source technologies and a version of Power BI; scaling up would require significant adaptations in terms of storage capacity, computing power and user management.

5.4. Perspectives

Several research and development avenues are emerging. The first involves expanding the prototype to a pilot deployment across all 35 health zones of Kinshasa, and then to other provinces of the DRC. This deployment would require scaling up, resource optimization, and a comprehensive training program for end users.

The second perspective is the integration of artificial intelligence models for predictive analytics (epidemic forecasting, resource needs estimation, early detection of stockouts). Approaches such as federated learning, combined with differential privacy and blockchain, offer security and privacy guarantees for the analysis of distributed health data.

The third perspective is the extension of the system to other sectors (animal health, environment) within the framework of the "One Digital Health" approach. The adoption of international standards (HL7 FHIR, common data models) would facilitate this interoperability.

The fourth perspective is a longitudinal evaluation, measuring the impact of the system on decisions made and health outcomes (reduction in mortality, improvement in vaccination coverage, optimization of resources).

Finally, deepening security, with the exploration of techniques such as homomorphic encryption for analyses that fully preserve confidentiality, would constitute a promising avenue of research.

6. CONCLUSION

This research proposed, implemented, and validated a secure medical data governance (MDG) model based on Business Intelligence, specifically adapted to the Kinshasa context. The SMGD-BI model combines a four-layer BI architecture with a *Security-by-Design framework* integrating encryption, hybrid access control, blockchain traceability, and differential anonymization. Experimental results and expert validation confirm the model's technical feasibility, security robustness, and operational relevance.

This work makes several scientific contributions: an integrated health data governance model in a PRFI context, a hybrid security architecture adapted to medical data, a mathematical formalization of data flows and bottlenecks, and a reproducible mixed-methods evaluation methodology. Operationally, the functional prototype, technical specifications, validated KPIs, and administrative governance framework provide a concrete roadmap for deploying the system across Kinshasa.

The limitations of this study (limited geographical scope, reliance on synthetic data, subjective assessment) open up promising avenues for future research, including large-scale deployment, integration of predictive artificial intelligence, national and regional interoperability, and longitudinal evaluation of the impact on public health. Ultimately, this work hopes to contribute to the digital transformation of the Congolese healthcare system and, more broadly, to the discussion on the governance of medical data in low- and middle-income countries.

REFERENCES

[1] Silva, D., Azevedo, J., Claro, I., Gomes, L., & Duque, J. (2025). The Importance of Business Intelligence and Power BI in the Management of Healthcare Systems - Case Study in Portugal. In *Intelligent Sustainable Systems - Selected Papers of WorldS4 2025* (pp. 138-147). Springer.

[2] Djamba, KJ, Havyarimana, V., Mbambazi, BP, & Niyongabo, J. (2025). E-Health Implementation in the Democratic Republic of the Congo: Current Position. *International Journal of Health Sciences* , 9, 210-222.

[3] Basivikidi , H., et al. (2026). Operationalizing One Digital Health and FAIR Data Principles for Disease Surveillance in a Low-Medium Income Country in Africa: Qualitative Study in the Democratic Republic of the Congo. *JMIR Medical Informatics* , 14, e93321.

[4] Dowo Ndjate, S. (2026). Integration of health information systems and decision-making efficiency: an empirical study of DHIS2 in the metropolis of Kinshasa. *International Journal of Scientific Research* , 4(2).

[5] Sarani, M., Jahangiri, K., Karami, M., & Honarvar, M. (2025). Enhancing epidemic preparedness: a data-driven system for managing respiratory infections. *BMC Infectious Diseases* , 25(1), 159.

[6] Malin, B.A., Yan, C., & Bonomi, L. (2026). Privacy and Security Throughout the Health Data Life Cycle: From Primary Care to Research Networks. *Annual Review of Biomedical Data Science* , 9, 47-67.

[7] Peffers, K., Tuunanen , T., Rothenberger, M.A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems* , 24(3), 45-77.

[8] Hevner, A.R., March, S.T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly* , 28(1), 75-105.

[9] Venable, J., Pries-Heje, J., & Baskerville, R. (2016). FEDS: a Framework for Evaluation in Design Science Research. *European Journal of Information Systems* , 25(1), 77-89.

[10] Kimball, R., & Ross, M. (2013). *The Data Warehouse Toolkit: The Definitive Guide to Dimensional Modeling* (3rd ed.). Wiley.

[11] Cochran, W. G. (1963). *Sampling Techniques* (2nd ed.). John Wiley & Sons.

[12] Little, J. D. C. (1961). A Proof for the Queuing Formula: L = λ W. *Operations Research* , 9(3), 383-387.

[13] Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika* , 16(3), 297-334.

[14] ISO/IEC 25010:2011. *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models* .

[15] Hanna, R. (2025). A Unified Health Data Platform: A Metadata-Driven, Mesh-Enabled Framework for Secure, High-Quality, and Collaborative Health Informatics. *BMJ Health & Care Informatics* , 32(Suppl 1), A1.

[16] Africa CDC. (2025). Africa Sets Course to Strengthen and Harmonize Health Data Governance. Africa Health ExCon 2025.

[17] Democratic Republic of Congo Digital Code Law. (2023). Ordinance-Law No. 23/010 of March 13, 2023, establishing the Digital Code.

[18] WHO. (2025). Health data governance in the age of artificial intelligence: policy imperatives for the WHO European Region.

[19] Granular Level Privacy Aware Access Control in Block Chain Based EHR Systems. (2025). IEEE.

[20] A privacy preserving medical data management framework using blockchain enabled encrypted role based access control. (2025). *Scientific Reports* , 15, 43864.

[21] Blockchain-based access control frameworks for healthcare. (2025). *Scientific Reports* .

[22] Nugraha, A.J., & Maulana, H. (2025). Business Intelligence-Based System to Enhance National Health Insurance Claim Reporting in Hospitals: Design and Optimization Approach. *Proceedings of the 8th International Conference on Informatics, Engineering, Science & Technology (INCITEST 2025)* .

[23] A Comprehensive Business Intelligence Framework for Diabetes Management in Telemedicine. (2026). *Systems* .

[24] Health- FedNet : A privacy-preserving federated learning framework for scalable and secure healthcare analytics. (2025). *ScienceDirect* .

[25] PriCollabAnalysis : privacy-preserving healthcare collaborative analysis on blockchain using homomorphic encryption and secure multiparty computation. (2025). *Springer* .

[26] Ethical AI in Healthcare: Integrating Zero-Knowledge Proofs and Smart Contracts for Transparent Data Governance. (2025). *Bioengineering* , 12(11), 1236.

[27] Enhancing Healthcare Security: A Unified RBAC and ABAC Risk-Aware Access Control Approach. (2025). *MDPI* .

[28] Securing Digital Health through Big Data Analytics and Blockchain Driven Cybersecurity in Healthcare Systems. (2025). IEEE Conference Proceedings.

[29] Toward blockchain based electronic health record management with fine grained attribute based encryption and decentralized storage mechanisms. (2025). *Scientific Reports* .

[30] Comparative Evaluation of K-Anonymity, Differential Privacy, and Pseudonymization for Data Protection in Rare Disease Registries. (2025).

[31] On the fidelity versus privacy and utility trade-off of synthetic patient data. (2025). *iScience* , 28(5), 112382.

[32] African Union Digital One Health Information Policy and Associated One Health Information Architecture Framework. (2025). AU-IBAR.

[33] Cultivating an equity-oriented data sharing culture for African health research initiatives. (2025). *Nature Communications* .

[34] A systematic review of tools cited in health information systems evaluations of developing and low to middle income countries. (2025). *Discover Public Health* .

[35] Co-design in quality management: developing a data-driven business intelligence dashboard for 14-day readmission at a Taiwan medical center. (2025). *BMJ Open Quality* .

[36] Short-User Experience Questionnaire (UEQ-S) for dashboard evaluation. (2025). *Publikasi Dinus* .

[37] Data protection, interoperability and governance assessment tool: results from a proof-of-concept survey. (2025). *Frontiers in Digital Health* , 7, 1685774.

[38] A rapid review on the application of common data models in healthcare: Recommendations for data governance and federated learning in artificial intelligence development. (2025). *PubMed* .

[39] Evaluating AI adoption in healthcare: Insights from the information governance professionals in the United Kingdom. (2025). *International Journal of Medical Informatics* , 199, 105909.

[40] Characterizing a Framework for Assessment of the Use of FAIR Principles for Health Data in Digital Health Devices Regulation. (2025). *Studies in Health Technology and Informatics* , 323, 270-274.

[41] Secure-DP FedMiner : A Lightweight Framework for Privacy-Preserving Data Mining Across Healthcare Institutions. (2025). *Library CNU* .

[42] Exploring the future of privacy-preserving heart disease prediction: a fully homomorphic encryption-driven logistic regression approach. (2025). *Journal of Big Data* .

[43] Blockchain-enabled secure Internet of Medical Things (IoMT) architecture for multi-modal data fusion in precision cancer diagnosis and continuous monitoring. (2025). *Scientific Reports* .

[44] MedAccessX : A Blockchain-Enabled Dynamic Access Control Framework for IoMT Networks. (2025). *Sensors* , 25(6), 1857.

[45] Real-Time ETL for EAV-Modeled Clinical Data: A CDC-Based Approach Using OpenMRS . (2026). *IEEE Xplore* .

[46] Design and Implementation of a Scalable Clinical Data Warehouse for Resource-Constrained Healthcare Systems. (2025). *IEEE Xplore* .

[47] Data Warehousing for Optimizing Healthcare Resource Allocation in Botswana. (2025). *HELINA 2025* .

[48] Power BI HIPAA-Compliant Healthcare Dashboards Implementation Playbook (2026). (2025). EPC Group.

[49] Ensuring General Data Protection Regulation Compliance and Security in a Clinical Data Warehouse From a University Hospital: Implementation Study. (2025). *ScienceDirect* .

[50] The Advanced Confidentiality Engine as a Scalable Tool for the Pseudonymization of Biomedical Data. (2025). *ScienceDirect* .

[51] Analytics Platform & DHIS2. (2026). DHIS2.

[52] Business Intelligence in Healthcare: Guide to Implementation. (2025). MADE IN.

[53] Healthcare Data Platform. (2025). GitHub.

[54] DermaDashboard : Bridging the Gap Between FHIR Standards and Clinical Usability. (2025). *ScienceDirect* .

[55] Designing a Data Mart at the Indonesian Psychological Healthcare Center Using Pentaho. (2025). *Semantic Scholar* .

[56] A real-time dashboard for optimizing blood product utilization through a FHIR-based data integration pipeline. (2025). *ScienceDirect* .

[57] Real-Time Vital Sign Monitoring of Contagious Diseases in West Africa's Healthcare System Using Grafana and IoT Devices. (2025). *Springer* .

[58] A Practical Framework for Encrypted Medical Prediction using Blockchain-Anchored Key Management System. (2025). *ACM* .

[59] Blockchain-Enabled Explainable AI for Trusted Healthcare Systems. (2025). *arXiv* .

[60] Adaptive Data Quality Management for Multi-Cloud Healthcare Warehouses: FHIR-Aware Semantics and Unsupervised Thresholding. (2025). *International Journal of AI and Data Science for ML* , 1(1).