Journal of Medical and Health Studies (JMHS)
ISSN: 2710-1452
DOI: 10.32996/jmhs
Journal Homepage: www.al-kindipublisher.com/index.php/jmhs

JMHS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Rule-Based Artificial Intelligence for Health Information Management, Governance, and Healthcare Quality

Shadaid Alanezi
Department of Health Information Management and Technology, College of Applied Medical Sciences, University of Hafr Al Batin, Hafr Al Batin 39524, Saudi Arabia
Corresponding Author: Shadaid Alanezi, **E-mail**: alanezishd@uhb.edu.sa

| ABSTRACT

Health information governance weaknesses can create operational risks in digital healthcare environments, including incomplete documentation, duplicate patient records, weak access control, poor interoperability, absent audit trails, and delayed reporting. These risks may affect data quality, information security, care continuity, accountability, reporting reliability, healthcare quality, and community-level planning. This paper proposes an artificial intelligence rule-based information governance framework for classifying such risks in health information management and health information systems. Using a scenario-based design-science approach, the framework defines governance input variables, maps them to health information management and health information system mechanisms, applies explicit IF-THEN rules, assigns risk classes, generates explanation traces, and produces governance recommendations. The framework is demonstrated through six synthetic scenarios covering duplicate records, unauthorized access, incomplete referral information, missing clinical documentation, weak audit trails, and delayed public health reporting. The demonstration shows how governance weaknesses can be converted into structured inputs, interpretable risk outputs, and corrective actions. The study does not claim empirical validation or deployment as a software system. Instead, it specifies a structured design artifact that can support future simulation, expert validation, rule-engine implementation, and empirical testing using real health information system data.

| KEYWORDS

Rule-Based Artificial Intelligence; Health Information Governance; Health Information Management; Health Information Systems; Healthcare Quality; Scenario-Based Analysis.

| ARTICLE INFORMATION

ACCEPTED: 21 April 2026 **PUBLISHED:** 08 May 2026 **DOI:** 10.32996/jmhs.2027.7.7.7

1. Introduction

Health information management and health information systems are central to digital healthcare delivery. Clinical documentation, patient identification, coding, referral management, reporting, quality monitoring, and public health planning depend on data that are accurate, complete, secure, timely, interoperable, traceable, and usable. When these conditions are weak, information problems can become operational risks, including fragmented records, delayed care, privacy exposure, poor reporting, and unreliable planning (Ghaffari Heshajin et al., 2024; Oecd, 2015; World Health, 2021; World Health Organization Regional Office for the Eastern, 2019).

Information governance provides the policies, standards, responsibilities, controls, and accountability mechanisms that regulate how health information is created, accessed, shared, protected, audited, retained, and used(Ghaffari Heshajin et al., 2024; Oecd, 2015). In practice, governance links health information management functions with health information system controls, including documentation quality, patient identity management, data quality monitoring, access control, authentication, authorization, audit logs, interoperability, and secure information exchange (Ghaffari Heshajin et al., 2024; National Institute of & Technology, 2024; Torab-Miandoab et al., 2023). The value of a health information system therefore depends not only on technical functionality, but also on whether governance rules are translated into reliable operational controls.

Healthcare information environments continue to face governance weaknesses such as incomplete documentation, duplicate records, unclear data ownership, weak access control, absent audit trails, poor interoperability, and delayed reporting. These weaknesses may reduce clinical reliability, weaken continuity of care, compromise privacy, limit accountability, and reduce the usefulness of data for quality improvement and community health planning (Kahn et al., 2016; Lewis et al., 2023; Syed et al., 2023; Torab-Miandoab et al., 2023; Weiskopf & Weng, 2013). Data quality is central to this problem because electronic health records are commonly assessed through completeness, correctness, plausibility, currency, consistency, validity, uniqueness, and fitness for use (Kahn et al., 2016; Weiskopf & Weng, 2013).

Rule-based artificial intelligence offers a practical way to formalize governance logic. Unlike black-box predictive models, rule-based artificial intelligence represents knowledge through explicit IF–THEN rules, making it suitable for risk classification and explanation traces(Forgy, 1982; Swartout, 1985). This approach fits health information governance because many governance problems are not prediction problems; they are rule-compliance, risk-classification, traceability, and control problems. Rule-based approaches have also been applied to electronic health record data quality assessment, supporting their relevance to health information governance contexts (Wang et al., 2020).

Although prior studies address health information governance, data quality, information security, interoperability, scenario-based analysis, and design-science research, these areas are often treated separately. Less attention has been given to an integrated information-systems framework that connects governance conditions to health information management and health information system mechanisms, rule-based risk classification, explanation traces, governance recommendations, and healthcare quality or community health implications (Hevner et al., 2004; Peffers et al., 2014; Reeder & Turner, 2011; Vollmar et al., 2015; Wieringa, 2014).

This paper proposes a scenario-supported artificial intelligence rule-based framework for health information governance risk classification in health information systems. The framework maps selected governance conditions to health information management and health information system mechanisms, classifies them into risk categories, and demonstrates the logic through six synthetic scenarios: duplicate records, unauthorized access, incomplete referral information, incomplete clinical documentation, weak audit trails, and delayed public health reporting. The study is positioned as a design artifact that specifies rule-based governance logic for future simulation, rule-engine implementation, expert validation, and empirical testing.

The paper makes three contributions. First, it integrates health information governance, health information management, health information systems, healthcare quality, and community health planning into a single rule-based risk classification framework. Second, it introduces an explainable rule-based artificial intelligence layer that converts governance weaknesses into IF–THEN classifications with explanation traces and recommendations. Third, it demonstrates the framework through structured synthetic scenarios, preparing it for future computational implementation and validation.

The remainder of the paper is organized as follows. Section 2 reviews the literature. Section 3 explains the methodology. Section 4 presents the proposed framework. Section 5 presents the results and findings through synthetic scenario demonstration. Section 6 discusses implications, limitations, and future validation. Section 7 concludes the paper.

2. Literature Review

2.1 Information Governance, Data Quality, and Health Information System Reliability

Health information management defines how health information should be documented, coded, protected, corrected, retained, and used, while health information systems provide the digital infrastructure for these functions. Information governance connects both domains through policies, standards, responsibilities, controls, and accountability mechanisms for managing health information across its lifecycle (Ghaffari Heshajin et al., 2024; Oecd, 2015; World Health, 2021; World Health Organization Regional Office for the Eastern, 2019).

Health information system reliability depends not only on technical functionality, but also on whether governance rules are embedded in operational controls. Documentation standards, data ownership, access rights, validation rules, audit logs, interoperability mechanisms, and reporting procedures determine whether health data are accurate, complete, secure, traceable, and fit for use (Ghaffari Heshajin et al., 2024; National Institute of & Technology, 2024; Oecd, 2015; Torab-Miandoab et al., 2023). Electronic health record data quality is commonly assessed through completeness, correctness, plausibility, currency, consistency, validity, uniqueness, accessibility, and fitness for use (Kahn et al., 2016; Lewis et al., 2023; Syed et al., 2023; Weiskopf & Weng, 2013). These dimensions directly affect clinical decision-making, patient identification, referral coordination, reporting, quality monitoring, and community health planning.

2.2 Security, Access Control, Auditability, and Interoperability

Security, privacy, access control, auditability, and interoperability are central governance mechanisms in health information systems. Healthcare organizations manage sensitive personal and clinical data, making authentication, authorization, access monitoring, and audit logging essential controls. Role-based access control assigns permissions according to organizational roles, while attribute-based access control allows decisions to consider user, resource, action, and contextual attributes (Hu et al.,

2014; Sandhu et al., 1996). Audit trails strengthen accountability by recording who accessed or modified data, when the action occurred, and what was changed (Ghaffari Heshajin et al., 2024; National Institute of & Technology, 2024; Oecd, 2015). Interoperability is also governance-dependent. Standards such as Fast Healthcare Interoperability Resources support structured health data exchange, but reliable interoperability also requires rules for data quality, patient identity, consent, access rights, sharing agreements, auditability, and accountability (International, 2019; Torab-Miandoab et al., 2023). Without such governance, connected systems may still exchange incomplete, delayed, poorly coded, or untrusted information. Data quality, access control, auditability, and interoperability therefore represent key mechanisms through which governance affects health information system reliability, healthcare service quality, and community-level planning.

2.3 Rule-Based Artificial Intelligence and Scenario-Based Governance Logic

Rule-based artificial intelligence represents knowledge through explicit IF–THEN rules. Unlike black-box predictive models, it is suitable when the problem involves governance logic, compliance checking, risk classification, explanation, and recommended action rather than statistical prediction (Swartout, 1985; Wang et al., 2020). Rule engines match facts against rule conditions; the Rete algorithm is a classic example of efficient many-rule and many-fact pattern matching (Forgy, 1982).

This logic fits health information governance because many governance requirements are rule-oriented. Access should match role or context, documentation should meet completeness requirements, audit trails should exist, referral data should include required fields, reports should be timely, and patient records should be unique. Such requirements can be formalized as rules that classify data quality, privacy, continuity-of-care, accountability, or reporting risks. Scenario-based analysis and design-science research provide a suitable methodological basis for developing such an artifact before full implementation or empirical validation(Hevner et al., 2004; Peffers et al., 2014; Reeder & Turner, 2011; Vollmar et al., 2015; Wieringa, 2014).

2.3 Research Gap

Prior literature provides foundations for health information governance, data quality, access control, interoperability, rule-based systems, scenario-based analysis, and design-science research. However, these areas are usually treated separately. Three gaps remain. First, limited work integrates governance conditions, health information management functions, health information system controls, and healthcare or community implications into one governance-to-risk logic. Second, rule-based artificial intelligence remains underused as an explainable mechanism for classifying information governance risks. Third, early-stage framework development still needs structured methods that can operate before access to real institutional data or system implementation.

To address these gaps, this paper proposes an artificial intelligence rule-based information governance framework for health information management and health information systems. The framework represents governance weaknesses as structured rule inputs and translates them into interpretable risk classifications, explanation traces, and governance recommendations.

3. Methodology

3.1 Research Design

This study adopts a scenario-based design-science approach supported by rule-based artificial intelligence logic. The purpose is to develop an information-systems artifact that translates selected health information governance conditions into risk classifications, explanation traces, and governance recommendations. The study is design-oriented rather than empirical; it does not test statistical associations, estimate causal effects, or validate the framework using real hospital data (Hevner et al., 2004; Peffers et al., 2014; Reeder & Turner, 2011; Vollmar et al., 2015; Wieringa, 2014).

The framework was developed in five steps: identifying governance dimensions from the literature, translating them into operational health information management and health information system variables, constructing synthetic governance scenarios, developing IF–THEN rules, and interpreting the outputs as plausible healthcare quality and community health implications. This approach is appropriate because many information governance requirements are rule-oriented, including documentation completeness, access control, authentication, auditability, interoperability, data quality monitoring, and reporting timeliness (Buchanan & Shortliffe, 1984; Ghaffari Heshajin et al., 2024; Hu et al., 2014; National Institute of & Technology, 2024; Oecd, 2015; Sandhu et al., 1996; Wang et al., 2020).

3.2 Governance Variables and Operationalization

The framework draws on literature in health information governance, data quality, cybersecurity governance, access control, interoperability, rule-based systems, scenario-based analysis, and design-science research (Forgy, 1982; Ghaffari Heshajin et al., 2024; Hu et al., 2014; National Institute of & Technology, 2024; Oecd, 2015; Sandhu et al., 1996; Torab-Miandoab et al., 2023; Wang et al., 2020; Weiskopf & Weng, 2013). The selected dimensions represent recurring risks in health information management and health information system environments and were operationalized as rule-readable variables.

Table 1. Governance dimensions and operational variables

Governance Dimension	*Operational Variable*	*Value Set*
Data ownership	Ownership clarity	Clear / Partial / Unclear
Documentation completeness	Completeness level	High / Moderate / Low
Data accuracy	Accuracy level	High / Moderate / Low
Patient identity management	Duplicate record status	Absent / Possible / Present
Access control	Access control strength	Strong / Moderate / Weak
Authentication	Authentication strength	Strong / Moderate / Weak
Authorization	Role alignment	Appropriate / Partial / Inappropriate
Auditability	Audit trail status	Complete / Partial / Absent
Interoperability	Interoperability level	Strong / Moderate / Weak
Reporting timeliness	Timeliness level	High / Moderate / Low
Data quality monitoring	Monitoring status	Active / Partial / Absent
Accountability	Correction responsibility	Defined / Partial / Undefined

These variables form the input space of the rule-based framework and allow governance weaknesses to be represented as structured conditions rather than narrative descriptions.

3.3 Rule-Based Classification Logic

The framework uses IF–THEN logic to classify governance risks. Each rule links governance and health information management / health information system conditions to a risk class, explanation trace, and governance recommendation:

IF governance condition A is present
AND HIM/HIS condition B is present
THEN risk classification = X
AND explanation trace = Y
AND governance recommendation = Z.

Each input condition is assigned a severity score: 0 for controlled conditions, 1 for partial or moderate weaknesses, and 2 for severe weaknesses. For example, clear ownership, high completeness, strong access control, complete audit trails, high reporting timeliness, active monitoring, and defined correction responsibility score 0. Partial, moderate, or possible conditions score 1. Unclear ownership, low completeness, weak access control, absent audit trails, low reporting timeliness, absent monitoring, undefined correction responsibility, or present duplicate records score 2.

Table 2. Risk scoring and classification scheme

Total Risk Score	*Risk Class*	*Interpretation*
0–2	Low	Governance condition is acceptable or controlled.
3–5	Moderate	Weakness exists but is limited or partially controlled.
6–8	High	Weakness may affect data quality, security, continuity, or reporting reliability.
≥9 or critical trigger	Critical	Weakness may seriously compromise privacy, accountability, patient safety, or community health planning.

A critical trigger is applied when a severe governance weakness directly affects privacy, patient safety, accountability, or public health response, such as absent audit trails with unauthorized access risk or missing allergy information in medication-related decisions. The scoring scheme is illustrative rather than empirically calibrated; it is used to make the rule logic explicit and reproducible for future simulation, expert validation, or rule-engine implementation.

3.4 Scenario Construction and Output Interpretation

Six synthetic scenarios were constructed to demonstrate the framework. They were selected because they represent common governance weaknesses across data quality, security, interoperability, auditability, and reporting.

Table 3. Scenario set used for framework demonstration

Scenario	*Governance Issue*	*HIM/HIS Problem*	*Main Risk Class*
S1	Weak data ownership	Duplicate patient records	Record integrity risk
S2	Weak access control	Unauthorized data access	Privacy and security risk
S3	Poor interoperability	Incomplete referral data	Continuity-of-care risk
S4	Incomplete documentation	Missing clinical information	Clinical decision-support risk
S5	Weak audit trail	No traceability of data changes	Accountability risk
S6	Delayed reporting	Late public health data aggregation	Community planning risk

Each scenario produces four outputs: risk classification, explanation trace, governance recommendation, and plausible healthcare quality or community health implication. The scenarios are synthetic, not empirical cases; they are used to demonstrate how the proposed rule logic represents plausible governance conditions consistently (Reeder & Turner, 2011; Vollmar et al., 2015).

3.5 Methodological Boundaries and Ethics

This study does not use patient-level data, hospital operational data, surveys, interviews, expert panels, institutional case studies, or system logs. No identifiable health information is collected, processed, analyzed, or reported. Therefore, the study does not involve direct human-subject research.

The framework is not presented as a deployed artificial intelligence system. It is an early-stage design artifact that specifies governance variables, rule logic, risk classes, explanation traces, and recommendations. Future work should validate the model through expert review, simulation, prototype rule-engine implementation, and empirical testing using real health information system data (Hevner et al., 2004; Peffers et al., 2014; Wieringa, 2014). Any future implementation should comply with relevant ethical, legal, institutional, privacy, and cybersecurity requirements (National Institute of & Technology, 2024).

4. Proposed AI Rule-Based Information Governance Framework

4.1 Framework Architecture

The proposed framework is a rule-based information-systems artifact for classifying health information governance risks. It translates selected governance conditions into risk outputs, explanation traces, and governance recommendations. The framework is not designed as a predictive machine-learning model; its purpose is to formalize governance logic in a transparent and auditable structure (Buchanan & Shortliffe, 1984; Forgy, 1982; Hevner et al., 2004; Peffers et al., 2014; Wang et al., 2020).

The framework consists of five connected layers. The first layer represents information governance conditions, including policies, responsibilities, standards, and accountability mechanisms related to data ownership, access, documentation, auditability, interoperability, and reporting. The second layer represents health information management mechanisms, including documentation quality, coding accuracy, patient identity management, record completeness, correction workflow, and data quality monitoring. The third layer represents health information system controls, including authentication, authorization, role-based or attribute-based access permissions, audit logs, validation rules, interoperability functions, reporting systems, and secure exchange mechanisms. The fourth layer represents rule-based artificial intelligence logic, where IF–THEN rules classify governance risks and generate explanation traces. The fifth layer represents outcome and recommendation outputs, including risk classes, governance recommendations, and plausible implications for healthcare quality and community health planning.

The core logic of the framework is:

Governance condition → HIM/HIS mechanism → Triggered rule → Risk classification → Explanation trace → Governance recommendation

This sequence makes the framework traceable because each output can be linked to the governance condition and health information management or health information system mechanism that triggered it.

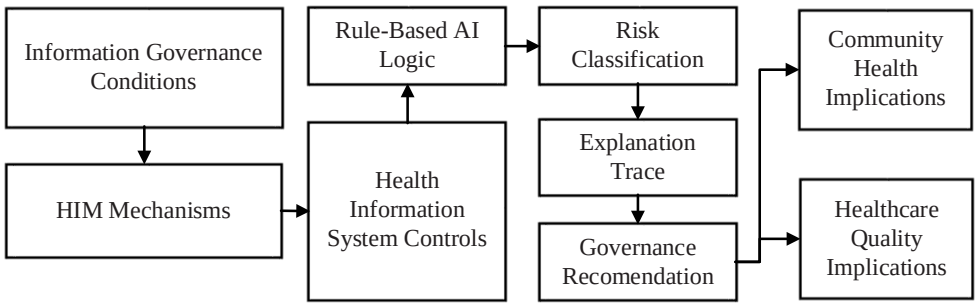

Figure 1. Layered architecture of the proposed AI rule-based information governance framework

4.2 Input Variables and Risk Logic

The framework uses the operational variables and scoring scheme defined in Section 3. These variables include ownership clarity, documentation completeness, data accuracy, duplicate record status, access control strength, authentication strength, role alignment, audit trail status, interoperability level, reporting timeliness, data quality monitoring, and correction responsibility. Within the framework, these variables function as rule-readable inputs. For example, **access control = weak, audit trail = absent, or interoperability = weak** can trigger one or more rule-based classifications. The purpose is not to estimate statistical risk, but to represent governance weaknesses in a structured and reproducible form.

4.3 Rule Structure

Each rule follows a consistent structure:
IF governance condition A is present
AND HIM/HIS condition B is present
THEN risk classification = X
AND explanation trace = Y
AND governance recommendation = Z.

For example:
IF access control = weak
AND audit trail = absent
THEN privacy and accountability risk = critical
AND explanation = unauthorized access cannot be reliably detected or traced
AND recommendation = implement role-based access control and audit-log monitoring.

The rules are grouped into five categories: data quality and record integrity, security and privacy, interoperability and continuity, auditability and accountability, and reporting and community planning. This categorization aligns the rule base with the main governance pathways through which health information systems may affect healthcare quality and community-level planning.

4.4 Rule Base

Table 4 presents the proposed rule base. The rules are not empirically calibrated; they are a structured design artifact intended for future validation, simulation, or implementation.

Table 4. Proposed rule base for health information governance risk classification

Rule ID	*Category*	*Rule Condition*	*Risk Output*	*Governance Recommendation*
R1	Data quality	IF completeness = low AND accuracy = low	Data quality risk = high	Apply validation rules and data quality review.
R2	Data quality	IF completeness = low AND clinical dependency = high	Decision-support risk = high	Enforce mandatory clinical documentation fields.
R3	Data quality	IF accuracy = low AND data quality monitoring = absent	Information reliability risk = high	Activate data quality monitoring and correction workflow.
R4	Record integrity	IF duplicate records = present AND identity management = weak	Record integrity risk = high	Strengthen patient identity management and duplicate detection.
R5	Record	IF duplicate records = present	Continuity-of-care risk	Consolidate records and assign

	integrity	AND clinical history is fragmented	= high	stewardship responsibility.
R6	Ownership	IF ownership clarity = unclear AND correction responsibility = undefined	Data stewardship risk = high	Define data owner and correction authority.
R7	Security	IF access control = weak AND authentication = weak	Security risk = high	Strengthen authentication and access control.
R8	Security	IF role alignment = inappropriate AND sensitive data access = broad	Unauthorized access risk = high	Enforce role-based or attribute-based access control.
R9	Privacy	IF unauthorized access is possible AND audit trail = absent	Privacy/accountability risk = critical	Implement audit logs and access monitoring.
R10	Privacy	IF access review = absent AND privileges are excessive	Confidentiality risk = high	Conduct periodic access privilege review.
R11	Auditability	IF audit trail = absent AND record modification is possible	Traceability risk = critical	Enable complete audit logging.
R12	Auditability	IF audit trail = partial AND incident investigation is required	Investigation support = weak	Improve log completeness and retention.
R13	Interoperability	IF interoperability = weak AND referral data = incomplete	Continuity-of-care risk = high	Standardize referral exchange and required fields.
R14	Interoperability	IF exchange delay = high AND specialist care depends on referral data	Service delay risk = high	Improve HIE workflow and referral data transfer.
R15	Interoperability	IF data standardization = weak AND systems exchange data	Semantic consistency risk = high	Adopt standardized data exchange formats.
R16	Reporting	IF reporting timeliness = low AND population data completeness = low	Community planning risk = high	Automate reporting and monitor completeness.
R17	Reporting	IF disease trend data = delayed AND planning requires current data	Public health response risk = critical	Define reporting deadlines and escalation rules.
R18	Monitoring	IF data quality monitoring = absent AND reporting depends on aggregated data	Reporting reliability risk = high	Implement data quality dashboard.
R19	Positive governance	IF accuracy = high AND access control = strong AND audit trail = complete	Governance support = strong	Maintain monitoring and periodic review.
R20	Positive interoperability	IF interoperability = strong AND referral data = complete	Continuity support = strong	Maintain exchange standards and workflow monitoring.

This rule base specifies rule categories, trigger conditions, risk outputs, and governance recommendations. It also prepares the framework for future implementation as a rule engine or governance dashboard.

4.5 Explanation Trace

The framework generates an explanation trace for each classification. The trace links the input condition to the triggered rule, risk class, explanation, and recommended governance action:

Input condition → Triggered rule → Risk class → Explanation → Governance recommendation

For example:

Input: access control = weak; audit trail = absent
Triggered rule: R9

Risk class: critical privacy/accountability risk
Explanation: unauthorized access cannot be reliably detected or traced
Recommendation: implement audit logs and access monitoring.

This traceability is important because health information governance requires decisions that are transparent, auditable, and defensible. It also distinguishes the framework from a general conceptual model because the reasoning path is explicit and can be reviewed, tested, refined, or implemented computationally.

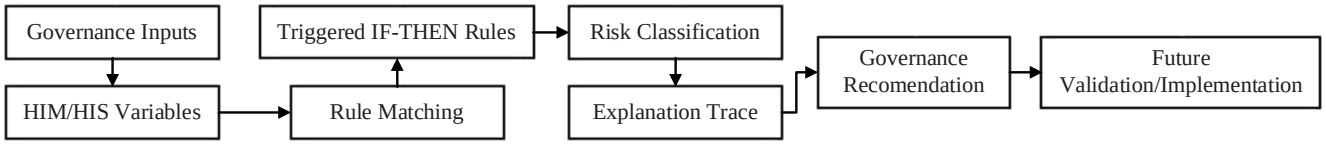

Figure 2. Rule-based inference flow for governance risk classification

4.6 Governance-to-Outcome Mapping

The framework links governance conditions to operational health information management and health information system mechanisms and outcome implications. Table 5 summarizes this mapping.

Table 5. Governance-to-outcome mapping

Governance Dimension	***HIM/HIS Mechanism***	***Rule-Based Risk Interpretation***	***Healthcare Quality Implication***	***Community Health Implication***
Data ownership	Data stewardship and correction workflow	Weak ownership increases correction risk.	Delayed correction of errors	Reduced trust in service reliability
Documentation completeness	Clinical documentation and record review	Low completeness increases decision risk.	Poor clinical decision-making	Weak service planning data
Data accuracy	Validation rules and data quality monitoring	Low accuracy increases information reliability risk.	Incorrect or delayed decisions	Weak planning based on unreliable data
Patient identity management	Duplicate detection and master patient index	Duplicate records increase integrity risk.	Fragmented care and repeated tests	Distorted population data
Access control	RBAC/ABAC permissions	Weak access control increases privacy risk.	Confidentiality risk	Lower public confidence
Authentication /authorization	User verification and privilege management	Weak authentication increases security risk.	Unauthorized data use	Reduced trust in digital health
Auditability	System logs and traceability	Absent audit trails increase accountability risk.	Weak incident investigation	Reduced institutional trust
Interoperability	Health information exchange	Poor interoperability increases continuity risk.	Referral delay and fragmented care	Delayed access to coordinated services
Reporting timeliness	Reporting systems and data aggregation	Low reporting timeliness reduces monitoring support.	Weak quality monitoring	Poor local health planning
Data sharing governance	Secure exchange and consent rules	Weak sharing governance increases misuse risk.	Unsafe or incomplete exchange	Reduced trust in data-driven services

4.7 Framework Operation

The framework operates in five steps. First, the governance condition is identified. Second, the affected health information management or health information system mechanism is mapped. Third, the relevant IF–THEN rule is triggered. Fourth, the risk is classified according to the scheme defined in Section 3. Fifth, the framework generates an explanation trace and governance recommendation.

This operation converts health information governance from a broad managerial concept into a structured rule-based classification model. It specifies how governance weaknesses can be represented as inputs, processed through explicit rules, and translated into interpretable outputs. The framework is therefore suitable for future testing through simulation, expert validation, prototype rule-engine implementation, or empirical evaluation using real health information system data (Hevner et al., 2004; Peffers et al., 2014; Wieringa, 2014).

4.8 Section Summary

This section presented the proposed AI rule-based information governance framework. The framework consists of governance inputs, health information management and health information system mechanisms, IF–THEN rules, risk classifications, explanation traces, and governance recommendations. Its main contribution is to formalize health information governance as a transparent rule-based risk classification model. The next section demonstrates the framework using synthetic governance scenarios.

5. Results/Findings: Framework Demonstration Using Synthetic Governance Scenarios

5.1 Demonstration Design

This section demonstrates the proposed artificial intelligence rule-based information governance framework using six synthetic governance scenarios. The purpose is to show how governance weaknesses can be represented as structured inputs, processed through IF–THEN rules, classified into risk categories, and linked to explanation traces and governance recommendations.
The scenarios are not empirical cases. They are synthetic cases designed to demonstrate the internal logic of the framework before future simulation, validation, or implementation. The six scenarios were selected because they represent common governance risks in health information management and health information systems: weak data ownership, weak access control, poor interoperability, incomplete documentation, weak audit trails, and delayed public health reporting (Ghaffari Heshajin et al., 2024; National Institute of & Technology, 2024; Oecd, 2015; Reeder & Turner, 2011; Torab-Miandoab et al., 2023; Vollmar et al., 2015).

5.2 Scenario Input Matrix

Table 6 presents the scenario input matrix used to demonstrate the framework. The table is presented in a transposed format to improve readability in A4 portrait layout. Each column represents one scenario, and each row represents a governance or health information management / health information system input variable used to trigger rule-based classification.

Table 6. Scenario input matrix

Variable	***S1: Duplicate records***	***S2: Unauthorized access***	***S3: Incomplete referral***	***S4: Missing documentation***	***S5: Weak audit trail***	***S6: Delayed reporting***
Ownership clarity	Unclear	Partial	Clear	Clear	Partial	Clear
Data completeness	Moderate	High	Low	Low	Moderate	Low
Access control	Moderate	Weak	Strong	Strong	Moderate	Strong
Authentication	Moderate	Weak	Strong	Strong	Moderate	Strong
Audit trail	Partial	Partial	Complete	Complete	Absent	Partial
Interoperability	Moderate	Moderate	Weak	Moderate	Moderate	Moderate
Reporting timeliness	Moderate	Moderate	Moderate	Moderate	Moderate	Low
Main triggered risk	Record integrity risk	Privacy/security risk	Continuity-of-care risk	Decision-support risk	Accountability risk	Community planning risk

Note. The table reports the operational input values assigned to each synthetic scenario. The transposed format is used to improve readability in A4 portrait layout while preserving the same scenario-level information. Each column represents one scenario, and each row represents a governance or health information management / health information system input variable used to trigger rule-based classification. The matrix converts narrative scenarios into rule-readable inputs. This improves reproducibility and prepares the framework for later rule-engine implementation.

5.3 Scenario-Specific Trigger Variables

Some rule outputs require additional trigger variables beyond the core input matrix. Table 7 specifies these scenario-specific conditions so that each classification is traceable to explicit inputs.

Table 7. Scenario-specific trigger variables

Scenario	*Scenario-Specific Trigger Variables*	*Main Triggered Rule Logic*
S1: Duplicate records	Duplicate records = present; identity management = weak; correction responsibility = undefined	Weak ownership + duplicate records + weak identity management
S2: Unauthorized access	Role alignment = inappropriate; access review = absent; sensitive data access = broad	Weak access control + weak authentication + role misalignment
S3: Incomplete referral	Referral data = incomplete; exchange delay = high; specialist care depends on referral data	Weak interoperability + incomplete referral data
S4: Missing documentation	Clinical dependency = high; allergy information = missing; mandatory fields = weak	Low completeness + high clinical dependency
S5: Weak audit trail	Record modification = possible; user activity logging = absent; incident investigation required = yes	Absent audit trail + untraceable record modification
S6: Delayed reporting	Population data completeness = low; disease trend data = delayed; local planning requires current data	Low reporting timeliness + incomplete population health data

This table makes the demonstration more transparent because each output can be traced to a defined condition or combination of conditions.

5.4 Rule-Based Scenario Outputs

Table 8 summarizes the triggered rule outputs, rule IDs, classification bases, risk classes, explanation traces, and governance recommendations for each scenario.

Table 8. Scenario output matrix

Scenario	*Triggered Rule Output*	*Rule ID(s)*	*Classification Basis*	*Risk Class*	*Explanation Trace*	*Governance Recommendation*
S1: Duplicate records	Record integrity risk	R4, R6	High-risk combination; no critical trigger	High	Unclear ownership + weak identity management + duplicate records	Assign data steward; activate duplicate detection; consolidate records
S2: Unauthorized access	Privacy/security risk	R7, R8, R10	High-risk combination; no critical trigger	High	Weak access control + weak authentication + role misalignment	Enforce RBAC/ABAC; strengthen authentication; review privileges
S3: Incomplete referral	Continuity-of-care risk	R13, R14	High-risk interoperability and referral-data weakness	High	Weak interoperability + incomplete referral data	Standardize referral exchange; require mandatory referral fields
S4: Missing documentation	Clinical decision-support risk	R2	Critical trigger if allergy data are missing in medication-related decisions	High/Critical	Low completeness + high clinical dependency; critical if allergy data are missing	Enforce mandatory fields; activate completeness alerts
S5: Weak audit trail	Accountability risk	R9, R11, R12	Critical trigger: absent audit trail with untraceable access or modification	High/Critical	Absent audit trail + untraceable record modification	Implement audit logging; monitor high-risk access and modification events
S6: Delayed	Community	R16,	High-risk reporting	High	Low reporting	Automate reporting;

reporting	planning risk	R17, R18	weakness; critical only if time-sensitive public health response is required		timeliness + incomplete population health data	monitor completeness; escalate delays

The output matrix shows that the framework classifies different governance weaknesses using a consistent logic. Each output is traceable from input condition to triggered rule, rule ID, classification basis, risk class, explanation, and recommendation.

5.5 Scenario Risk Profile

To summarize the scenario outputs visually, Figure 3 presents a risk-profile heatmap across five governance risk categories: data quality, security/privacy, interoperability, auditability, and reporting/community planning.
The heatmap uses a four-level scale: **1 = low, 2 = moderate, 3 = high, and 4 = critical**.

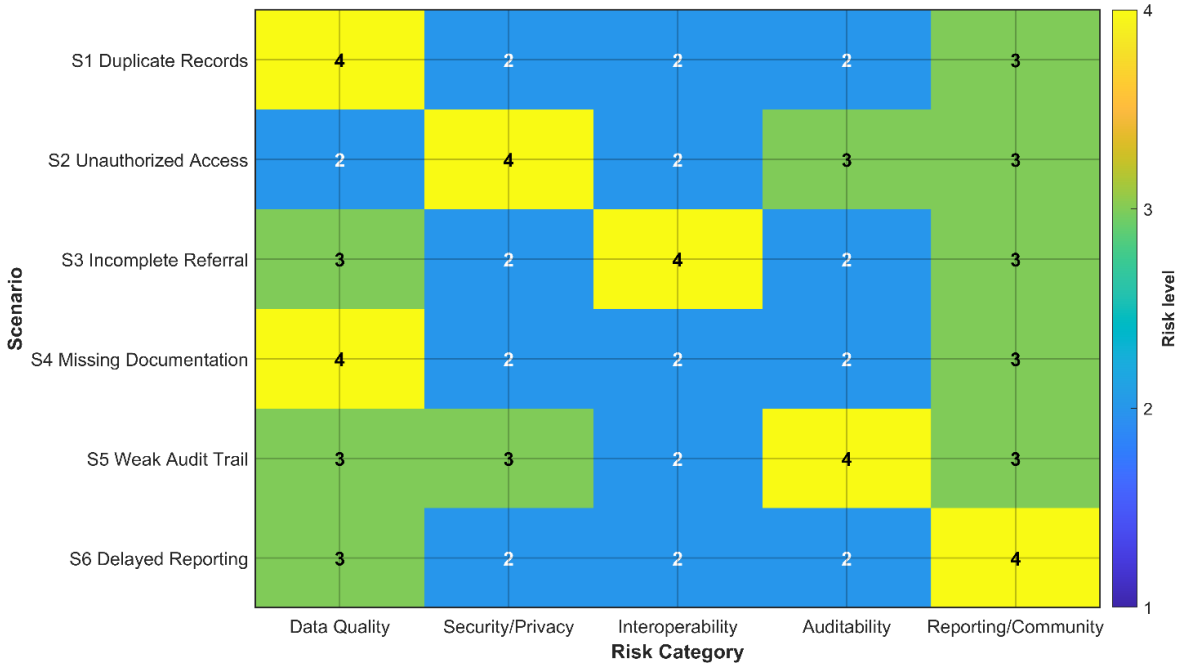

Figure 3. Scenario risk profile across governance risk categories. Values represent conceptual rule-based risk classifications: 1 = low, 2 = moderate, 3 = high, and 4 = critical.

Table 9. Risk-profile values used for Figure 3

Scenario	*Data Quality*	*Security /Privacy*	*Interoperability*	*Auditability*	*Reporting /Community*
S1: Duplicate records	4	2	2	2	3
S2: Unauthorized access	2	4	2	3	3
S3: Incomplete referral	3	2	4	2	3
S4: Missing documentation	4	2	2	2	3
S5: Weak audit trail	3	3	2	4	3
S6: Delayed reporting	3	2	2	2	4

These values are conceptual risk classifications derived from the framework logic. They are not statistically estimated risk scores.

5.6 Interpretation of Demonstration Results

The demonstration shows that information governance weaknesses can be represented as structured inputs and classified through explicit rule logic. Weak data ownership primarily produces record-integrity risk. Weak access control produces privacy

and security risk. Poor interoperability produces continuity-of-care risk. Incomplete documentation produces decision-support and patient-safety risk. Weak auditability produces accountability risk. Delayed reporting produces community-planning risk.
The results also show that health information management and health information system mechanisms are interdependent. Health information management defines documentation quality, patient identity management, record completeness, and data stewardship, while health information systems implement these requirements through validation rules, access controls, audit logs, interoperability mechanisms, and reporting systems. The rule-based layer links both domains by converting governance conditions into interpretable risk classifications.
The demonstration should be interpreted as a structured demonstration of framework logic, not as empirical validation. It shows that the framework can organize governance weaknesses, classify risks, generate explanation traces, and suggest governance actions. Future work should test the rule base using expert validation, simulation, prototype implementation, or real health information system data (Hevner et al., 2004; Peffers et al., 2014; Wieringa, 2014).

5.7 Section Summary

This section demonstrated the proposed framework using six synthetic governance scenarios. The demonstration converted governance weaknesses into structured input variables, scenario-specific triggers, rule IDs, risk classifications, explanation traces, and governance recommendations. By replacing narrative scenarios with input–output matrices and a risk-profile visualization, the section shows the framework's practical logic more directly and prepares it for future simulation, validation, and computational implementation.

6. Discussion

6.1 Principal Contribution

This study developed a scenario-based artificial intelligence rule-based framework for classifying health information governance risks in health information management and health information systems. Its main contribution is the formalization of governance logic into structured inputs, IF–THEN rules, risk classifications, explanation traces, and governance recommendations.
The framework addresses a practical gap in health information systems research. Governance weaknesses such as duplicate records, weak access control, incomplete documentation, absent audit trails, poor interoperability, and delayed reporting are often treated as administrative or quality-management problems. This study reframes them as rule-classifiable information-system risks by connecting governance conditions to health information management mechanisms, health information system controls, risk outputs, and plausible healthcare quality or community health implications.
The scenario demonstration also strengthens the methodological contribution. Rather than using scenarios as narrative examples, the study treats them as structured synthetic cases with input variables, scenario-specific triggers, rule outputs, risk classes, explanation traces, and recommendations. This makes the framework more suitable for future simulation, rule-engine implementation, expert validation, and empirical testing.

6.2 Implications for Health Information Management and Health Information System Governance

The framework reinforces the role of health information management as a governance function rather than a purely administrative record-management activity. Documentation quality, coding accuracy, patient identity management, data correction, privacy control, retention, and data quality monitoring are operational points where governance becomes visible. When these functions are weak, information risks emerge: incomplete documentation weakens decision support, unclear ownership contributes to duplicate records, and poor correction workflows allow inaccurate information to persist (Ghaffari Heshajin et al., 2024; Kahn et al., 2016; Lewis et al., 2023; Syed et al., 2023; Weiskopf & Weng, 2013).
For health information system design, the framework shows that governance should be embedded into system controls. Access control, authentication, authorization, audit logging, validation rules, duplicate record detection, interoperability functions, and reporting workflows are not only technical features; they are mechanisms for enforcing governance requirements (Ghaffari Heshajin et al., 2024; Hu et al., 2014; International, 2019; National Institute of & Technology, 2024; Oecd, 2015; Sandhu et al., 1996). The rule-based artificial intelligence layer provides a practical way to represent these controls. Weak access control combined with absent audit trails can trigger privacy and accountability risk; weak interoperability combined with incomplete referral data can trigger continuity-of-care risk; and duplicate records combined with weak patient identity management can trigger record-integrity risk. These outputs are useful because they identify both the risk and the conditions that produced it.

6.3 Implications for Healthcare Quality and Community Planning

The framework conceptualizes healthcare quality as partly dependent on the reliability of the health information environment. Safe, timely, efficient, and continuous care requires data that are complete, accurate, secure, traceable, and available when needed (Institute of, 2001) (Institute of Medicine, 2001). The scenario demonstration shows plausible pathways through which duplicate records, incomplete documentation, poor interoperability, weak audit trails, and delayed reporting may affect clinical decisions, referral continuity, accountability, quality monitoring, and planning.

These pathways suggest that healthcare quality improvement should include information governance controls as part of quality infrastructure. Clinical protocols, staffing, workflow redesign, and patient experience initiatives may be limited if the underlying data are incomplete, delayed, insecure, or poorly governed. Data quality monitoring, access governance, auditability, interoperability, and reporting reliability should therefore be treated as quality-enabling mechanisms, not merely technical or compliance concerns (Ghaffari Heshajin et al., 2024; Kahn et al., 2016; Lewis et al., 2023; Syed et al., 2023).

At the community level, the framework makes a narrower claim. It does not argue that information governance directly improves community health. Rather, it argues that governance improves the data conditions needed for community health planning, surveillance, prevention, reporting, and resource allocation (World Health, 2021; World Health Organization Regional Office for the Eastern, 2019). In this sense, governance functions as an enabling infrastructure for community health improvement.

6.4 Value of Rule-Based Artificial Intelligence for Governance Risk Classification

The value of rule-based artificial intelligence in this study lies in explainability. Many healthcare artificial intelligence applications focus on prediction, diagnosis, or analytics and depend on large datasets and model training. By contrast, the problem addressed here is governance classification. Governance requirements are naturally rule-based: access should match role or context, documentation should meet completeness requirements, audit trails should exist, referral data should include required fields, and reports should be submitted on time.

A rule-based structure makes governance reasoning explicit. It can show which condition triggered a risk classification, why the risk level was assigned, and what governance action is recommended. This is important in health information governance, where privacy, accountability, auditability, and defensibility are central requirements (Buchanan & Shortliffe, 1984; Forgy, 1982; Wang et al., 2020). The framework should not be interpreted as a deployed artificial intelligence system; it is a design artifact that specifies logic for future rule-engine implementation.

6.5 Limitations and Future Validation

This study has clear limitations. It does not use patient-level data, hospital operational data, surveys, interviews, expert panels, institutional case studies, or system logs. The scenarios are synthetic and do not measure the frequency, severity, or organizational impact of governance weaknesses. The rule base is not yet implemented in a software prototype or evaluated in a rule engine, and the risk scores are illustrative rather than empirically calibrated.

Future research should expand and formally specify the rule base, including thresholds, rule priorities, and conflict-resolution logic. The framework should also be implemented as a prototype rule engine or governance dashboard and tested through simulation, expert validation, and empirical case studies using real health information system data, audit logs, data quality reports, incident reports, and governance documents (Hevner et al., 2004; Peffers et al., 2014; Wieringa, 2014).

7. Conclusion

This paper proposed an artificial intelligence rule-based information governance framework for health information management and health information systems. The framework formalizes common governance weaknesses, including incomplete documentation, duplicate records, weak access control, poor interoperability, absent audit trails, and delayed reporting, as operational risks affecting data quality, security, care continuity, accountability, reporting reliability, and community planning. Its main contribution is a rule-based risk classification model that maps governance conditions to health information management and health information system mechanisms, applies IF–THEN rules, assigns risk classes, generates explanation traces, and produces governance recommendations. This structure makes governance logic transparent, auditable, and suitable for future rule-engine or dashboard implementation.

The synthetic scenarios demonstrated how the framework classifies six risks: record integrity, privacy and security, continuity of care, decision support, accountability, and community planning. They show how governance weaknesses can be converted into structured inputs, interpretable outputs, and corrective actions.

The study remains conceptual. It does not use real hospital data, has not yet been empirically validated, and the rule base has not yet been implemented. Future work should expand the rule base, define rule priorities, implement a prototype dashboard, and test the framework using simulated and real health information system data. Overall, the framework provides an explainable foundation for developing more accountable, secure, interoperable, and quality-oriented health information systems.

Statements and Declarations

Funding: This research received no external funding. The APC was not externally funded.

Conflicts of Interest: The author declares no conflict of interest.

Ethics Approval: This study did not involve human participants, human material, patient records, hospital operational data, surveys, interviews, or identifiable health information. Therefore, formal ethics approval was not required.

Data Availability: No empirical datasets were generated or analyzed during the current study. The framework demonstration is based on synthetic scenarios developed for conceptual and methodological illustration.

Acknowledgments: Not applicable.

ORCID iD: Shadaid Alanezi: 0009-0002-6667-5150.

Publisher's Note: All claims expressed in this article are solely those of the author and do not necessarily represent those of the affiliated organization, or those of the publisher, the editors, and the reviewers.

References

[1]. Buchanan, B. G., & Shortliffe, E. H. (1984). *Rule based expert systems: the mycin experiments of the stanford heuristic programming project (the Addison-Wesley series in artificial intelligence)*. Addison-Wesley Longman Publishing Co., Inc.
[2]. Forgy, C. L. (1982). Rete: A fast algorithm for the many pattern/many object pattern match problem. *Artificial Intelligence*, *19*(1), 17-37. https://doi.org/10.1016/0004-3702(82)90020-0
[3]. Ghaffari Heshajin, S., Sedghi, S., Panahi, S., & Takian, A. (2024). A framework for health information governance: a scoping review. *Health Res Policy Syst*, *22*(1), 109. https://doi.org/10.1186/s12961-024-01193-9
[4]. Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, *28*(1), 75-105.
[5]. Hu, V. C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R., & Scarfone, K. (2014). *Guide to Attribute Based Access Control (ABAC) Definition and Considerations* [NIST Special Publication 800-162].
[6]. Institute of, M. (2001). *Crossing the Quality Chasm: A New Health System for the 21st Century*. National Academies Press.
[7]. International, H. L. (2019). FHIR Release 4: Fast Healthcare Interoperability Resources Specification.
[8]. Kahn, M. G., Callahan, T. J., Barnard, J., Bauck, A. E., Brown, J., Davidson, B. N.,…Schilling, L. (2016). A Harmonized Data Quality Assessment Terminology and Framework for the Secondary Use of Electronic Health Record Data. *EGEMS (Wash DC)*, *4*(1), 1244. https://doi.org/10.13063/2327-9214.1244
[9]. Lewis, A. E., Weiskopf, N., Abrams, Z. B., Foraker, R., Lai, A. M., Payne, P. R. O., & Gupta, A. (2023). Electronic health record data quality assessment and tools: a systematic review. *J Am Med Inform Assoc*, *30*(10), 1730-1740. https://doi.org/10.1093/jamia/ocad120
[10]. National Institute of, S., & Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* [NIST CSWP 29].
[11]. Oecd. (2015). *Health Data Governance*. OECD Publishing. https://doi.org/10.1787/9789264244566-en
[12]. Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2014). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45-77. https://doi.org/10.2753/mis0742-1222240302
[13]. Reeder, B., & Turner, A. M. (2011). Scenario-based design: a method for connecting information system design with public health operations and emergency management. *J Biomed Inform*, *44*(6), 978-988. https://doi.org/10.1016/j.jbi.2011.07.004
[14]. Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *Computer*, *29*(2), 38-47. https://doi.org/10.1109/2.485845
[15]. Swartout, W. R. (1985). *Rule-based expert systems: The mycin experiments of the stanford heuristic programming project: BG Buchanan and EH Shortliffe,(Addison-Wesley, Reading, MA, 1984); 702 pages, $40.50*. Elsevier.
[16]. Syed, R., Eden, R., Makasi, T., Chukwudi, I., Mamudu, A., Kamalpour, M.,…Myers, T. (2023). Digital Health Data Quality Issues: Systematic Review. *J Med Internet Res*, *25*, e42615. https://doi.org/10.2196/42615
[17]. Torab-Miandoab, A., Samad-Soltani, T., Jodati, A., & Rezaei-Hachesu, P. (2023). Interoperability of heterogeneous health information systems: a systematic literature review. *BMC Med Inform Decis Mak*, *23*(1), 18. https://doi.org/10.1186/s12911-023-02115-5
[18]. Vollmar, H. C., Ostermann, T., & Redaelli, M. (2015). Using the scenario method in the context of health and health care--a scoping review. *BMC Med Res Methodol*, *15*, 89. https://doi.org/10.1186/s12874-015-0083-1
[19]. Wang, Z., Talburt, J. R., Wu, N., Dagtas, S., & Zozus, M. N. (2020). A Rule-Based Data Quality Assessment System for Electronic Health Record Data. *Appl Clin Inform*, *11*(4), 622-634. https://doi.org/10.1055/s-0040-1715567
[20]. Weiskopf, N. G., & Weng, C. (2013). Methods and dimensions of electronic health record data quality assessment: enabling reuse for clinical research. *J Am Med Inform Assoc*, *20*(1), 144-151. https://doi.org/10.1136/amiajnl-2011-000681
[21]. Wieringa, R. J. (2014). *Design Science Methodology for Information Systems and Software Engineering*. Springer. https://doi.org/10.1007/978-3-662-43839-8
[22]. World Health, O. (2021). *Global Strategy on Digital Health 2020-2025*.
[23]. World Health Organization Regional Office for the Eastern, M. (2019). *Eastern Mediterranean Region: Framework for Health Information Systems and Core Indicators for Monitoring Health Situation and Health System Performance 2018*.