Health Information Governance and Regulatory Compliance: Comparative Frameworks for Data Verification, Risk Screening, and Confidentiality in Health and Financial Systems

Sylviastella Favour Peteranaba[1*], Helen Ekwi Osinem[2], Florence Eribenne[3], Olakunle Saheed Soyege[4]

[1]Independent Researcher, Favourpeteranaba@gmail.com
[2]Jos University Teaching Hospital (JUTH), Nursing Services Department, Jos, Nigeria helenosinem@gmail.com
[3]Bay Cove Human Services, Boston, MA, USA, feribenne1980@gmail.com
[4]Independent Researcher, Pretoria, south Africa, ossoyege@gmail.com

*Corresponding Author: Sylviastella Favour Peteranaba, Favourpeteranaba@gmail.com

Abstract

This review examines the governance and regulatory mechanisms that shape the collection, verification, use, protection, and exchange of sensitive information across health and financial systems. Its purpose is to clarify shared compliance principles, identify sector-specific risks, and evaluate how verification, screening, confidentiality, and accountability can be strengthened within increasingly digital environments. The study adopts a structured comparative review approach, synthesizing multidisciplinary literature on health information governance, financial compliance, privacy regulation, identity management, data quality, risk monitoring, breach response, and regulatory harmonization. The findings show that both sectors depend on reliable data quality, traceable records, validated identities, proportionate risk screening, controlled access, and auditable decision processes. However, differences in legal mandates, operational priorities, and information flows create distinct compliance challenges, particularly in relation to secondary data use, customer due diligence, public-health surveillance, cross-border transfers, and third-party processing. The review further demonstrates that digital transformation expands the compliance perimeter through cloud services, artificial intelligence, mobile platforms, distributed architectures, and automated decision systems, thereby increasing demands for privacy-by-design, continuous monitoring, model validation, and incident readiness. It concludes that effective governance requires the coordinated integration of law, technology, institutional capability, professional competence, and continuous oversight rather than isolated technical or legal controls. The study recommends interoperable regulatory standards, stronger cross-border cooperation, workforce development, transparent data-sharing rules, tested breach-response mechanisms, periodic validation of automated screening tools, and greater accountability for third-party processors. Future research should prioritize implementation outcomes across jurisdictions, especially in emerging economies, and assess whether harmonized governance frameworks can improve compliance consistency while preserving legitimate access, innovation, operational resilience, and public trust across rapidly evolving interconnected digital ecosystems.

Keywords: Information governance; Regulatory compliance; Data verification; Risk screening; Confidentiality; Digital transformation.

1. Introduction

1.1 Information Governance and Regulatory Context

Information governance has become a component of institutional accountability because contemporary health and financial systems depend on large volumes of data. In healthcare, governance determines how information is generated, validated, accessed, shared, retained, and protected across clinical, administrative, and public-health environments. Nigeria's experience illustrates why governance structures matter: fragmentation among health-information institutions, weak coordination, and absent data-management governance mechanisms can impair the reliability and usefulness of national information systems (Meribole et al., 2018). Governance must therefore be understood as an institutional architecture linking data quality, stewardship, accountability, interoperability, and lawful processing rather than as a narrow information-technology function.

The regulatory context converts ethical expectations concerning confidentiality and information use into enforceable organizational obligations. Digital health has widened the range of actors that create or process health information, including hospitals, insurers, laboratories, technology vendors, applications, and remote-monitoring platforms. This expansion complicates assumptions that sensitive medical information remains inside a bounded clinical environment. Effective regulation consequently requires transparent rules for authorization, secondary use, disclosure, security safeguards, and accountability across data ecosystems (Rockwern et al., 2021). These requirements are especially important when data move between organizations or are repurposed for analytics, research, insurance assessment, or automated decision-making.

Regulatory models differ across jurisdictions. Within Europe, the General Data Protection Regulation established privacy, accountability, transparency, fairness, purpose limitation, and data-subject rights as elements of data governance. Yet the expansion of digital health has exposed tensions between formal consent mechanisms, conventional regulatory categories, and emerging uses of health data at scale (Marelli, Lievevrouw & Van Hoyweghen, 2020). Compliance therefore cannot be reduced to consent or privacy notices; it requires assessment of whether institutional practices remain compatible with technological capabilities and the substantive rights regulation seeks to protect.

African regulatory environments reveal comparable pressures and institutional constraints. In South Africa, implementation of the Protection of Personal Information Act has highlighted the need to balance stronger protection of personal health information with legitimate uses for patient care, surveillance, research, and public health. Stakeholders have emphasized data quality, transparency, accountability, and understanding of data-protection duties as conditions for effective implementation (Staunton, Tschigg & Sherman, 2021). Statutory compliance thus depends on organizational capability and procedures capable of translating legal principles into routine information-management practices.

Governance effectiveness is also shaped by leadership and implementation capacity. Regulatory frameworks may be sophisticated yet produce weak outcomes where institutions lack ethical leadership, coordinated execution, or mechanisms ensuring that formal requirements influence operational behaviour. Evidence from the Southern African Development Community context

emphasizes ethical leadership in technological transformation and policy implementation, reinforcing the proposition that governance quality depends on accountable institutional actors as much as written rules (Enaifoghe, Dlamini & Agwuna, 2020). This is relevant to information stewardship, where confidentiality and verification controls require managerial ownership.

Financial systems offer a useful comparative domain because compliance similarly depends on identification, traceable information flows, monitoring, and controlled disclosure. Anti-money-laundering and counter-terrorist-financing requirements compel financial institutions to collect, verify, analyse, and report customer and transactional information, creating tensions among commercial priorities, customer relationships, privacy expectations, and reporting duties (Ball et al., 2020). The comparison with healthcare is instructive: both sectors manage sensitive data, operate under confidentiality expectations, and must justify information sharing through legal, risk-management, or public-interest purposes.

Technology is embedded within this regulatory infrastructure. In banking, regulatory technology can support transaction monitoring, compliance analysis, and anti-money-laundering controls, demonstrating how automated systems strengthen risk screening while creating new requirements for model oversight, data integrity, auditability, and human accountability (Turki et al., 2020). Comparable developments in health systems include automated validation, interoperable records, decision-support technologies, and digitally mediated access controls, making governance inseparable from the design and supervision of information-processing technologies.

At the international level, information governance increasingly emphasizes harmonization without assuming identical national laws. Cross-border health data use requires frameworks that preserve privacy and security while enabling legitimate access, interoperability, research, quality improvement, and public-interest analysis. The OECD positions health-data governance around coordinated national frameworks, transparent processing, data quality, security protections, and international cooperation, while recognizing differences in implementation maturity across countries (OECD, 2022). Within a comparative health-financial perspective, this context establishes the basis for examining verification, risk screening, confidentiality, accountability, and controlled data exchange as mutually reinforcing governance functions.

1.2 Cross-Sector Compliance Challenges and Risks

Cross-sector regulatory compliance increasingly operates within information environments in which health providers, financial institutions, technology vendors, insurers, public agencies, and outsourced partners exchange sensitive data across organizational boundaries. The resulting risk is not confined to unauthorized disclosure; it encompasses inaccurate verification, fragmented accountability, inconsistent retention practices, weak auditability, and uncertainty regarding responsibility when data are reused or transferred. Nigeria's evolving data-protection architecture illustrates this complexity because general privacy rules coexist with sector-specific requirements, creating compliance obligations that organizations must interpret across overlapping legal and institutional arrangements (Babalola, 2022).

Comparable difficulties arise in African financial systems where rapid digitization increases efficiency and exposure to cyber-enabled misuse. South Africa's experience demonstrates that institutions must reconcile consumer-data protection with operational demands, cross-border processing, cybersecurity and alignment between domestic rules and external regimes such as the GDPR. These pressures make regulatory compliance an ongoing governance function rather than a periodic legal exercise, particularly where financial services depend on interconnected platforms and third-party data processing (Warikandwa, 2021).

Health systems face parallel vulnerabilities because electronic records aggregate clinical, demographic, diagnostic, and administrative information whose compromise can affect privacy, institutional trust, and patient safety. Security deficiencies may arise from unauthorized access, weak authentication, insider misuse, insecure transmission, heterogeneous systems, and inadequate technical safeguards. Consequently, compliance risk extends beyond formal observance of privacy rules to the capacity to preserve confidentiality, integrity, availability, and appropriate access throughout the information lifecycle (Keshta & Odeh, 2021).

Financial-data governance demonstrates how regulatory design can generate different balances between information sharing and individual protection. Consumer credit systems require accurate identification and reliable data exchange to support lending and risk assessment, yet expansive collection may intensify surveillance, exclusion, or misuse when safeguards are weak. Variations among credit-data regimes reveal that regulatory outcomes depend on institutional design, allocation of responsibilities, access rules, and mechanisms for correcting or contesting information (Mizrahi-Borohovich & Levi-Faur, 2020).

Across both sectors, compliance capability depends on competence. Distributed operations can produce inconsistent practices when staff capabilities, procedures, technological skills, and accountability structures vary across units or locations. Capability-building frameworks emphasizing competency alignment, continuous learning, workforce analytics, and coordinated performance management are relevant to compliance resilience, because regulatory controls ultimately depend on personnel who can interpret requirements and execute them consistently (Falemi, Akhigbe & Akin-Oluyomi, 2020). Cross-sector risk is shaped by the interaction of regulation, technology, data quality, capability, and institutional oversight.

1.3 Review Aim, Scope, and Objectives

This review examines the governance and regulatory structures that shape the verification, screening, protection, and responsible use of sensitive information across health and financial systems. Its central aim is to compare how both sectors manage data quality, confidentiality, risk detection, accountability, and regulatory compliance within increasingly digital and interconnected environments. By bringing these domains into a common analytical frame, the review seeks to identify areas of convergence, sector-specific differences, and transferable governance practices that can strengthen institutional resilience and public trust.

The scope encompasses information governance principles, regulatory obligations, data verification processes, identity and record validation, risk-screening mechanisms, confidentiality safeguards, access controls, monitoring practices, and breach-response arrangements. Particular attention is

given to the ways organizational structures, technological systems, professional responsibilities, and legal requirements interact to influence compliance outcomes. The review also considers the implications of cross-border data flows, third-party processing, automation, interoperable platforms, and emerging digital infrastructures that complicate traditional models of information stewardship.

The objectives are to clarify the conceptual foundations of health information governance; examine the regulatory expectations applicable to sensitive data management; compare verification, screening, and confidentiality mechanisms across health and financial contexts; assess the operational risks that arise when governance controls are fragmented or inconsistently applied; and identify opportunities for harmonized, adaptive, and technology-responsive compliance frameworks. The review further aims to highlight research, policy, and implementation priorities capable of improving transparency, accountability, data integrity, and secure information exchange while preserving legitimate access and institutional functionality. In doing so, it establishes a structured basis for evaluating governance effectiveness across sectors under evolving regulatory and technological conditions globally.

2. Foundations of Health Information Governance

2.1 Data Quality, Integrity, and Verification

Data quality, integrity, and verification form the evidentiary foundation of effective information governance because health and financial institutions increasingly depend on digitized records to support consequential decisions. Reliable information must be accurate, complete, timely, consistent, relevant, traceable, and sufficiently secure for its intended purpose. Within digital health environments, information-quality frameworks demonstrate that quality is multidimensional and must be assessed across the complete information lifecycle rather than treated merely as the absence of entry errors (Fadahunsi et al., 2021). Similar expectations apply in financial systems, where deficiencies in customer, transactional, or risk data may undermine identification procedures, credit decisions, fraud detection, regulatory reporting, and compliance monitoring.

Verification provides the procedural means through which institutions establish whether information is credible enough to support operational or regulatory action. Electronic health-record research identifies completeness, correctness, concordance, plausibility, and currency as important dimensions of quality assessment, supported by techniques including source comparison, validity checks, distributional analysis, agreement testing, and record review (Weiskopf & Weng, 2013). These principles are readily applicable across regulated sectors because neither a clinical decision nor a financial risk classification should depend on information whose provenance or internal consistency cannot be demonstrated.

Table 1. Comparative Data Quality, Integrity, and Verification Framework

Governance dimension	Health-system application	Financial-system application	Principal control mechanism
Accuracy	Correct diagnoses, demographics, and clinical observations	Correct customer and transaction information	Source validation and reconciliation

Completeness	Required clinical and administrative fields	Complete KYC and transaction records	Mandatory-field and exception checks
Consistency	Agreement across records and facilities	Agreement across accounts and platforms	Cross-system validation
Timeliness	Current patient and surveillance information	Current customer and risk information	Real-time or scheduled updating
Integrity	Protection against unauthorized record alteration	Protection against transaction manipulation	Access controls and audit trails
Verification	Confirmation of clinical or administrative data	Confirmation of identity and financial records	Authentication and authoritative-source checks
Monitoring	Detection of anomalous health-data patterns	Detection of abnormal transactions	Automated alerts and trend analysis
Traceability	History of record creation and modification	History of transactions and data amendments	Provenance logs and tamper-evident records

The challenges become particularly evident within resource-constrained health systems. Evidence across Eastern and Southern Africa demonstrates that routine health-information platforms may contain extreme values, temporal inconsistencies, mismatches between related indicators, and unreliable denominator information. Such deficiencies can compromise planning and surveillance even when electronic reporting systems are widely deployed (Maïga et al., 2019). Governance arrangements must therefore incorporate routine validation, feedback mechanisms, transparent correction procedures, and accountability for data quality at both collection and reporting levels.

Quality assurance begins at the point where information is generated. Public-health information systems require competent personnel, standardized procedures, appropriately configured technologies, organizational support, and clearly defined quality responsibilities. Errors introduced during initial collection can propagate through aggregation, analytics, interoperability platforms, and regulatory reporting, thereby magnifying their institutional consequences. Preventive validation and continuous quality control are therefore more effective than relying solely on retrospective correction after information has already influenced decisions (Chen et al., 2020).

Automated verification introduces further possibilities and responsibilities. Nigerian research on mammographic analysis illustrates how computational techniques can support systematic identification of clinically significant image features. Such applications demonstrate the value of automation but simultaneously reinforce the importance of source-data quality, appropriate reference criteria, algorithm validation, and professional oversight where computational outputs influence health-related judgments (Ejofodomi et al., 2014).

Measurement validity is equally important where governance systems rely upon scores, screening instruments, questionnaires, or classification models. Instrument-development research demonstrates the importance of reliability testing, construct validity, contextual adaptation, and

empirical validation before information is regarded as sufficiently dependable for interpretation (Sabboh, 2022). These principles are transferable to customer-risk models, patient-screening tools, compliance questionnaires, and automated decision systems.

Continuous monitoring can further strengthen information reliability. Statistical process-control principles distinguish normal variation from potentially significant deviations through repeated measurement, control thresholds, trend identification, and corrective action. Within governance systems, analogous mechanisms can identify duplicate records, missing values, unusual coding patterns, abnormal transactions, or unexpected changes before they become embedded in institutional reporting (Akanbi, Ganiu & Sunday, 2022).

Integrity finally requires assurance that verified information remains protected from undocumented alteration after capture. Distributed-ledger models demonstrate how cryptographic validation, traceable transactions, consensus mechanisms, and immutable histories can strengthen confidence in records exchanged among multiple participants (Shittu et al., 2021). For health and financial governance, these mechanisms underscore the importance of authenticated amendments, explicit provenance, controlled access, and comprehensive audit trails. Data quality and integrity must therefore be treated as continuous governance responsibilities connecting reliable capture, verification, monitoring, accountability, and defensible regulatory decision-making.

2.2 Risk Screening and Compliance Controls

Risk screening is a core information-governance function because institutions must distinguish ordinary activity from conditions requiring enhanced review, intervention, documentation, or escalation. In health and financial systems, effective screening depends on defined risk indicators, validated data, proportional thresholds, and controls that translate identified risk into accountable action. South Africa's anti-money-laundering framework illustrates this risk-based logic by requiring accountable institutions to establish risk-management and compliance programmes that support customer identification, verification, ongoing due diligence, and differentiated controls according to assessed exposure (Henning & Hauman, 2017).

A defensible screening architecture should recognize that risk rarely arises from a single variable. Nigerian predictor research demonstrates how multiple contextual and individual factors can be assessed jointly rather than interpreted in isolation, allowing institutions to distinguish relative contributions and combined effects within a defined population (Balogun & Sabboh, 2021). For governance systems, the transferable principle is that screening models should combine relevant variables while preserving transparency regarding why particular indicators alter a risk classification.

Risk assessment must also account for economic and contextual change. Evidence examining psychosocial predictors under depressed economic conditions demonstrates the value of analysing how changing circumstances affect observed outcomes rather than assuming that established relationships remain stable across environments (Ezeani & Sabboh, 2021). Health and financial compliance controls similarly require periodic recalibration where economic conditions, service-delivery models, fraud patterns, customer behaviour, or technological environments change.

The quality of screening further depends on selecting indicators that are conceptually connected to the outcome being assessed. Research on parenting styles and effortful control demonstrates the methodological importance of specifying predictors in advance, measuring them systematically, and testing their explanatory contribution (Oyarekua & Sabboh, 2021). In regulated environments, analogous discipline reduces arbitrary profiling and supports explainable, evidence-based risk categorisation.

Screening mechanisms must additionally address behavioural and ethical dimensions. Predictor-based analysis of moral disengagement illustrates how institutions can examine antecedent conditions associated with departures from expected norms (Sabboh, 2021). Applied to compliance, this supports attention to behavioural warning indicators, conflicts of interest, policy circumvention, unusual access activity, and other signals that may warrant investigation without treating any single indicator as determinative.

Environmental influences are equally relevant. Research relating school climate, self-efficacy, social media, and peer pressure to behavioural outcomes demonstrates how multiple external and internal factors may interact within risk assessment (Sabboh & Alausa, 2021). Cross-sector controls should consequently combine transactional or clinical indicators with contextual information while avoiding excessive data collection that is disproportionate to regulatory purpose.

Predictive screening also requires reliable instruments. Studies examining teaching styles and parental bonding through validated measures and regression-based analysis highlight the need for consistent measurement procedures before risk relationships are inferred (Sabboh & Olugbade, 2021). Compliance systems should therefore document data sources, scoring logic, validation intervals, false-positive rates, and human-review requirements.

Risk controls must be especially rigorous when screening concerns vulnerable populations or sensitive information. Predictor research involving psychosocial variables underscores the importance of validated instruments, responsible interpretation, and avoiding unsupported inference from correlational relationships (Sabboh & Yusuf, 2021). These principles parallel requirements for fairness, proportionality, confidentiality, and oversight in health-risk stratification and financial customer screening.

Finally, risk-screening systems should differentiate correlation from actionable evidence. Psychological-factor research demonstrates that statistically associated variables may assist structured assessment but require contextual interpretation before decisions are made (Yusuf & Sabboh, 2021). Accordingly, robust compliance controls should integrate automated alerts with documented human review, escalation protocols, audit trails, periodic model validation, and mechanisms for correcting erroneous classifications, ensuring that screening remains evidence-based, proportionate, and accountable across diverse institutions, jurisdictions, and changing regulatory environments where both under-screening and over-screening can generate operational consequences.

2.3 Confidentiality, Privacy, and Access Governance

Confidentiality, privacy, and access governance constitute interdependent components of responsible information management in health and financial systems. Confidentiality requires institutions to prevent inappropriate disclosure, privacy protects individuals against unjustified collection or use of personal information, while access governance determines which authenticated actors may view, modify, transmit, or reuse data. Increasing digitization has complicated these obligations because sensitive information now travels across organizational, technological, and jurisdictional boundaries. International experience in healthcare demonstrates that electronic records, analytics, interoperable systems, and third-party processing expand potential access points and therefore require stronger accountability, minimum-necessary access, secure transmission, and governance of secondary data use (Gatchalian, Kandy & Sattler, 2022).

Access control operationalizes these principles by transforming privacy requirements into enforceable system permissions. Risk-sensitive healthcare architectures demonstrate that authorization decisions can incorporate user roles, contextual circumstances, sensitivity classifications, and estimated disclosure risk rather than relying entirely upon static permissions (Shi et al., 2020). This approach is especially relevant where clinicians, researchers, administrators, insurers, and external partners require different levels of access to the same information environment.

Table 2. Comparative Confidentiality, Privacy, and Access Governance Controls

Governance dimension	Health-system application	Financial-system application	Principal control mechanism
Confidentiality	Protect clinical and patient information	Protect customer and transaction information	Encryption and disclosure controls
Privacy	Limit unjustified collection and reuse	Control use of personal financial data	Consent and purpose limitation
Authentication	Verify clinicians and authorized personnel	Verify customers and institutional users	Multi-factor authentication
Authorization	Restrict access by clinical role	Restrict access by operational responsibility	Role- or risk-based access control
Data sharing	Govern research and care exchanges	Govern banking and fintech exchanges	Controlled interfaces and agreements
Auditability	Record access and clinical amendments	Record transactions and data changes	Immutable logs and audit trails
Revocation	Withdraw inappropriate privileges	Revoke customer or third-party access	Privilege review and access termination
Accountability	Assign responsibility for data handling	Assign responsibility for financial records	Governance oversight and monitoring

Legal frameworks determine when access and processing are permissible. South Africa's Protection of Personal Information Act demonstrates the complexity of reconciling privacy protection with legitimate health research, particularly where consent, lawful processing, and institutional

responsibility intersect (Swales, 2022). Comparable challenges arise whenever confidentiality must coexist with public-health surveillance, regulatory reporting, research, or continuity of care.

Financial systems face similar pressures as open-banking arrangements permit information exchange among banks, fintech firms, and authorized service providers. Effective governance therefore requires meaningful control over transparency, portability, correction, consent, revocation, and subsequent data use so that expanded interoperability does not become uncontrolled circulation of financial information (Asrow, 2022).

Technological safeguards must reinforce these institutional and legal requirements. Secure distributed architectures demonstrate how cryptographic validation, permissioned participation, traceability, non-repudiation, and auditable transaction histories can strengthen information exchange across multiple actors (Shittu et al., 2022). Across both sectors, effective governance consequently depends on authenticated access, segregation of duties, encryption, periodic privilege review, auditable modifications, and clearly assigned responsibility for approving, monitoring, and terminating access to sensitive information.

3. Comparative Regulatory Frameworks Across Sectors

3.1 Health Data Regulation and Compliance Obligations

Health data regulation operates at the intersection of privacy law, clinical ethics, public-health authority, cybersecurity, and institutional accountability. Its purpose is not merely to restrict disclosure, but to establish conditions under which identifiable health information may be collected, verified, accessed, used, transferred, retained, and ultimately disposed of. In Nigeria, digital contact-tracing debates during COVID-19 demonstrated this balance clearly: public-health surveillance could be strengthened through mobile positioning data, yet implementation still required conformity with national privacy rules, proportionality, safeguards against misuse, and clearly defined purposes for processing personal information (Ekong, Chukwu & Chukwu, 2020). Regulatory compliance therefore requires both lawful authority and operational controls capable of translating legal principles into everyday data practices.

The compliance burden becomes more complex when health information moves beyond traditional clinical records. Patient-generated health data from wearable devices, mobile applications, consumer platforms, and technology companies can fall across overlapping regulatory regimes, creating uncertainty concerning who controls the data, which privacy protections apply, and whether information collected outside conventional healthcare settings receives protections comparable to clinical data. Regulatory fragmentation can consequently produce gaps between innovation and accountability, particularly when data are reused for analytics, commercial services, or algorithmic decision-making (Winter & Davidson, 2022). Health organizations must therefore map data flows, identify controllers and processors, establish lawful purposes, and determine applicable obligations before information enters interoperable or externally managed environments.

Consent remains important, but it cannot function as the sole basis of health-data governance. Comparative legal analysis shows that modern data-protection frameworks frequently permit health research processing under multiple lawful grounds and may provide specific research exemptions or safeguards. Treating consent as universally determinative can confuse ethical consent to

participate in research with legal authorization for processing personal data. Institutions must instead document the applicable lawful basis, observe purpose limitation and data minimization, implement safeguards for sensitive information, and preserve mechanisms through which individuals can exercise relevant data rights (Dove & Chen, 2020). These requirements make compliance a continuing governance responsibility rather than a one-time authorization event.

Figure 1. Health Data Regulation and Compliance Obligations Pathway

Lawful Basis and Purpose Specification
↓
Data Collection and Verification
↓
Identity, Authentication and Access Control
↓
Authorized Use, Sharing and Secondary Processing
↓
Security, Retention and Breach Management
↓
Audit, Accountability and Regulatory Review
↺ Continuous Risk Assessment, Training and Control Improvement

Cross-cutting obligations: confidentiality • transparency • data minimization • proportionality • data-subject rights • documented accountability

Cross-border research introduces additional obligations because legal expectations concerning anonymization, pseudonymization, consent, controller responsibility, and international transfer differ substantially among jurisdictions. Comparative examination of frameworks in Europe, the United States, Canada, Australia, and Switzerland demonstrates that inconsistent legislative requirements can impede multisite health research even where scientific collaboration is legitimate. Effective compliance therefore depends on standardized agreements, ethics oversight, transfer safeguards, privacy-enhancing technologies, and clear allocation of responsibility between organizations sharing health information (Scheibner et al., 2020). Regulatory interoperability is thus as important as technical interoperability when health datasets move between institutions or countries.

Public-health emergencies further test the proportionality of regulatory systems. During COVID-19, South Africa adopted extensive governmental measures involving surveillance, screening, restrictions, and coordinated health-system responses under conditions of rapidly evolving risk. Such circumstances illustrate the broader governance challenge of enabling timely public-health action while maintaining transparent institutional authority, defined responsibilities, and safeguards against unnecessary or indefinite expansion of exceptional measures (Ikwegbue et al., 2021). Emergency necessity should therefore alter neither the requirement for accountability nor the need to reassess intrusive data practices when the justification for them changes.

Figure 1 conceptualizes these obligations as a continuous compliance pathway rather than isolated legal checkpoints. Collection should begin with lawful authority and transparent purpose

specification; verification should establish accuracy and provenance; access should be limited according to role and necessity; use and sharing should remain compatible with authorized purposes; security controls should protect confidentiality and integrity; and breach management should provide containment, documentation, notification, and remediation. Oversight then closes the cycle through audit, risk review, policy revision, workforce training, and evidence of compliance.

Across this pathway, health institutions require demonstrable accountability. Policies must specify who may authorize processing, how identity and access are verified, when secondary use is permissible, how long information is retained, and what procedures govern correction, deletion, incident escalation, and third-party access. Regulators increasingly expect organizations not only to possess written policies but also to demonstrate that controls operate effectively in practice. The resulting compliance model integrates law, ethics, technology, documentation, and organizational responsibility, allowing health information to support care, research, surveillance, and system planning without weakening confidentiality, individual rights, or institutional trust across complex systems.

3.2 Financial Data Verification and Confidentiality Requirements

Financial data verification and confidentiality are complementary regulatory obligations because institutions must establish who a customer is, whether information is reliable, and how sensitive records may be used after verification. In Nigeria, banking privacy is shaped by the need to reconcile data use with protections against unauthorized possession, disclosure, or exploitation of personal information. Effective confidentiality requires lawful collection, purpose limitation, secure storage, controlled disclosure, and remedies where information is mishandled (Abdulkadir & Sambo, 2022).

Verification is central to customer due diligence. Evidence from Kenyan commercial banks shows that KYC compliance depends on obtaining identification documents, maintaining auditable evidence of due diligence, validating customer information, and ensuring staff competence and technological capacity. Weak verification can expose institutions to impersonation, fraud, money laundering, sanctions breaches, and inaccurate risk classification, while excessive procedures can impede access to financial services (Arasa & Ottichilo, 2015).

Digital identity infrastructures are increasingly used to address these tensions. Financial-sector identity systems can improve authentication, portability, and repeated verification by replacing fragmented analogue processes with standardized digital credentials. Yet greater connectivity also increases exposure to cyber risk, unauthorized profiling, and cross-jurisdictional uncertainty. Governance must therefore balance efficiency with market integrity, inclusion, cybersecurity, and responsibility for the accuracy and provenance of identity attributes (Arner et al., 2019).

Privacy-preserving electronic KYC offers a more integrated model. Blockchain-supported self-sovereign identity frameworks can enable customers to present verifiable credentials without placing unnecessary personal information on immutable ledgers. Such designs reduce duplicated data stores and facilitate selective disclosure, but their compliance value depends on trusted credential issuers, secure wallets, revocation mechanisms, interoperability, and architectures that preserve deletion and data-protection rights where legally required (Schlatt et al., 2022).

Verification also extends beyond customer identity to the reliability of financial information used for institutional and policy decisions. Analysis of monetary-policy rules across middle-income emerging economies demonstrates how financial judgments depend on measurable indicators, model specification, and consistent interpretation of economic data (Agwuna, Irrshad & Mazorodze, 2022). For regulated institutions, customer, transaction, risk, and reporting data require provenance, reconciliation, validation, and review before informing decisions. Confidentiality controls should operate across the lifecycle through encryption, role-based access, segregation of duties, logging, secure transmission, retention limits, and controlled disposal. Together, verification and confidentiality create an evidentiary chain in which data are authentic, appropriately restricted, traceable through authorized use, and capable of supporting defensible compliance reporting without unnecessary exposure.

4. Cross-Sector Governance and Compliance Mechanisms

4.1 Identity Verification and Record Validation

Identity verification and record validation are foundational controls in information governance because errors in establishing who a person is, or in linking records to the correct individual, can propagate through clinical care, financial transactions, regulatory reporting, and risk assessment. Effective governance therefore requires more than collecting identifiers; institutions must establish authoritative sources, validation rules, exception procedures, audit trails, and accountability for correcting mismatches. Governance models developed for distributed Nigerian operations illustrate the value of standardized data controls, transparent accountability, compliance monitoring, and quality assurance where information is exchanged across units (Akin-Oluyomi & Akhigbe, 2022).

In health systems, patient identification is consequential because duplicate records may fragment medical histories, distort surveillance, and associate clinical information with the wrong person. South African evidence shows that the absence of a universal identifier can impede de-duplication of routine laboratory data and weaken monitoring of prevention programmes. The use of an existing child-health identifier demonstrated how persistent identifiers can strengthen longitudinal linkage, provided that identifiers are consistently captured and validated across services (Haeri Mazanderani et al., 2018). This principle parallels financial customer identification, where stable identifiers reduce ambiguity but still require documentary or digital verification.

Record validation requires structured linkage rather than reliance on a single demographic field. In England, routine linkage between primary-care and external health datasets uses combinations of NHS number, date of birth, postcode, and gender, with validity flags, duplicate removal, match-ranking metadata, and governance controls surrounding identifiable information. Such multilayered procedures demonstrate that defensible matching depends on identifier quality and transparent documentation of linkage strength, eligibility, and possible misclassification (Padmanabhan et al., 2019). Similar controls apply to financial institutions when reconciling customer profiles across accounts, subsidiaries, payment platforms, and compliance databases.

Where exact identifiers are unavailable or inconsistent, probabilistic and machine-learning approaches can improve record matching. Australian research on supervised meta-ensemble linkage demonstrates that combining algorithms can improve precision and discrimination when records

contain inconsistencies, spelling variations, or incomplete attributes. Nevertheless, algorithmic matching creates governance responsibilities concerning threshold selection, false matches, missed matches, explainability, and periodic performance validation (Vo, Jonnagaddala & Liaw, 2019). Automated linkage should therefore generate confidence measures rather than transform uncertain identity relationships into unquestioned facts.

Digital identity architectures can reduce repeated verification while strengthening user control. A decentralized healthcare identity framework shows how blockchain-supported identities can authenticate patients and providers across remote-health environments while reducing dependence on centralized identity stores. The model emphasizes interoperable credentials, privacy preservation, user-controlled authorization, and secure verification, features increasingly relevant as healthcare interactions move beyond physical facilities (Javed et al., 2021). Their value depends on trustworthy enrollment because technically secure credentials can reproduce errors introduced during identity proofing.

Financial systems confront an analogous challenge through Know Your Customer requirements. Distributed-ledger approaches to KYC propose that validated customer information can be shared or reused among authorized institutions, reducing repetitive verification while maintaining traceability. Such models may improve efficiency, but require standards for credential issuance, data quality, permissioning, updates, revocation, and responsibility when verified information becomes inaccurate (Parra Moyano & Ross, 2017). Record validation must therefore remain continuous rather than ending after account opening.

Validation also benefits from anomaly-detection logic. Sensor-based monitoring research in Nigeria demonstrates how continuous comparison of observed data against expected operating conditions can identify deviations, faults, and unreliable inputs before they compromise overall system performance. Translated into health and financial information governance, the same principle supports automated detection of duplicate identities, incompatible demographic fields, unusual amendments, inconsistent identifiers, and records that depart from established validation rules (Sunday & Omoegun, 2020). Human review remains essential where exceptions have consequences.

4.2 Risk Screening, Monitoring, and Escalation

Risk screening, monitoring, and escalation form a control cycle through which health and financial institutions identify threats, assess significance, and direct exceptional cases toward proportionate intervention. Screening establishes an initial risk profile; monitoring tests whether transactions, clinical indicators, or access patterns depart from expected conditions; escalation determines when anomalies require human review, enhanced controls, reporting, or urgent action. This cycle depends on reliable data, thresholds, documented responsibilities, and feedback mechanisms that allow controls to adapt as risks change.

Predictive monitoring shifts institutional attention from responding after failure toward identifying precursors before harm occurs. Nigerian work on predictive maintenance demonstrates how sensor streams, historical patterns, condition indicators, and analytical models can support early identification of deterioration and prioritize intervention according to risk (Sunday et al., 2020). In

health governance, comparable logic can support deterioration alerts or anomalous record access; in finance, it can support suspicious-transaction monitoring and fraud detection.

Control systems must distinguish meaningful deviation from ordinary variability. Research on thermodynamic control strategies illustrates comparing observed performance with expected parameters and adjusting responses when conditions exceed acceptable ranges (Sunday et al., 2019). Risk governance similarly requires calibrated thresholds, because overly sensitive rules create false positives and investigation burden, whereas permissive thresholds may leave material threats undetected.

Integrated quality and reliability approaches show that monitoring is strongest when statistical surveillance is connected to corrective action rather than passive observation. Combining process-improvement and reliability principles supports failure analysis, risk prioritization, performance measurement, and intervention planning, providing a transferable architecture for compliance controls (Olutimehin & Ganiu, 2022).

Financial monitoring increasingly depends on computational screening of transactions. Evidence from mobile-money fraud prediction involving Ghanaian researchers demonstrates that machine-learning classifiers can identify suspicious patterns within imbalanced datasets, while precision, recall, and related measures remain essential for evaluating detection quality (Botchey, Qin & Hughes-Lartey, 2020). Such systems require governance over training data, thresholds, model drift, and investigator review.

More broadly, anomaly-detection research in financial fraud shows that supervised, semi-supervised, and unsupervised techniques can expose transactions or behaviours that differ materially from established patterns (Hilal, Gadsden & Yawney, 2022). Escalation should therefore be tiered according to severity, confidence, recurrence, and potential harm, with higher-risk cases triggering verification, restricted access, specialist review, incident documentation, or regulatory reporting. Audit trails should record alerts, decisions, overrides, and outcomes so institutions can evaluate false positives, missed events, response timeliness, and control effectiveness.

4.3 Confidentiality Safeguards and Breach Response

Confidentiality safeguards are effective only when organizations combine preventive controls with a rehearsed response capability for incidents that defeat those controls. In health and financial systems, breaches may involve unauthorized disclosure, alteration, destruction, loss, or unavailability of sensitive records, creating legal, operational, reputational, and patient-safety consequences. Privacy-by-design research therefore supports embedding minimization, access restriction, encryption, secure defaults, accountability, and lifecycle controls into information systems before deployment rather than treating confidentiality as a corrective requirement after exposure occurs (Semantha et al., 2020).

Human behaviour remains a critical exposure point. Evidence from a South African district hospital found patient-identifying information within clinical WhatsApp exchanges, demonstrating how ordinary communication practices can bypass formal safeguards even when used for legitimate coordination. Governance should consequently extend beyond core databases to messaging

applications, mobile devices, screenshots, exports, and informal channels through clear policies, workforce training, approved platforms, and proportionate monitoring (Meyer, Meyer et al., 2021).

Breach response begins with rapid recognition and disciplined escalation. A healthcare incident-response review identified managerial and technical strategies involving preparation, detection, containment, communication, recovery, learning, and coordination. Institutions should define incident severity levels, establish multidisciplinary response teams, preserve evidence, isolate compromised systems, maintain service continuity, and document decision-making so that response actions are auditable and proportionate to affected data and services (Jalali et al., 2019).

Regulatory notification is equally important. French breach-notification evidence showed that confidentiality loss was the dominant category among health-sector reports and highlighted potential underreporting where cybersecurity and privacy responsibilities are poorly aligned. Effective governance requires organizations to assess the nature and scale of exposure, identify affected individuals and systems, determine applicable notification duties, and maintain breach registers supporting supervisory review and post-incident remediation (Simon & Looten, 2020).

Resilience principles from Nigerian infrastructure research further emphasize layered protection, fault containment, safe system design, and restoration after abnormal conditions. Applied to information governance, these principles support segmentation, redundancy, backup integrity, controlled failover, and tested recovery procedures that prevent a localized compromise from becoming a system-wide failure (Adeniji et al., 2020). Confidentiality governance should therefore integrate prevention, detection, containment, notification, recovery, root-cause analysis, and corrective action within one accountable lifecycle. Post-breach reviews should verify whether access permissions, encryption, logging, vendor controls, retention practices, and staff procedures remain adequate, ensuring incident experience is converted into measurable improvements in institutional control maturity.

5. Emerging Challenges and Governance Priorities

5.1 Digital Transformation and Evolving Compliance Risks

Digital transformation is reshaping health and financial information governance by moving regulated activities from bounded institutional systems into interconnected ecosystems of cloud platforms, mobile applications, artificial intelligence, distributed databases, automated workflows, and third-party services. These technologies expand the speed and scale at which sensitive information can be collected, linked, analyzed, and exchanged, but they also enlarge the compliance perimeter. In health systems, the transition toward Health 4.0 alters established trust relationships by placing digital intermediaries between patients, professionals, institutions, and regulators, creating new questions concerning accountability, transparency, consent, and responsibility when technology participates directly in decision-making (Guckert et al., 2022).

African digital-health expansion illustrates the dual character of transformation. Across sub-Saharan Africa, mobile connectivity, digital platforms, artificial intelligence, and data-driven health services offer opportunities to extend access and address infrastructure shortages. However, rapid deployment can outpace governance capacity, particularly where interoperability, workforce capability, data protection, and institutional readiness remain uneven. Sustainable transformation

therefore requires regulatory arrangements addressing privacy, security, and local implementation rather than treating technological adoption as an independent objective (Holst et al., 2020).

Comparable tensions appear in financial services, where automation can strengthen compliance while generating new dependencies. Regulatory technology can standardize monitoring, reporting, data aggregation, and prudential workflows, allowing institutions to process complex obligations rapidly. Yet fragmented implementation can create duplicated systems, inconsistent data definitions, opaque models, and operational vulnerabilities. Integrating RegTech into broader digital-transformation strategies is consequently important because regulatory controls must remain aligned with business processes, risk management, and supervisory expectations rather than functioning as isolated technical tools (von Solms, 2021).

The governance implications of automation are also evident in industrial control environments. Nigerian research using the Siemens TIA Portal shows that integrated automation can synchronize real-time information and improve operational responsiveness across connected systems. From a compliance perspective, the same integration that enhances visibility can increase dependence on system configuration, access permissions, software integrity, interoperability, and reliable audit records. Automated environments therefore require change management, privileged-access controls, configuration validation, logging, and responsibility for decisions embedded within digital workflows (Sunday & Omoegun, 2022).

Digital transformation also involves connecting previously separate infrastructures. Research on integrating solar technologies into Nigerian manufacturing emphasizes technical capacity, financing, policy coordination, and organizational readiness when introducing new technology. These conditions are relevant to regulated health and financial systems: introducing cloud services, digital identity, remote monitoring, or automated analytics without corresponding governance capacity may create unmanaged interfaces, unclear ownership, and compliance gaps between legacy and newly deployed systems (Sunday & Omoegun, 2018).

Integration risk becomes more pronounced when multiple infrastructures operate as one system. Modeling hydrogen integration into national electricity grids demonstrates how interoperability, data gaps, uncertainty, regulatory environments, and coordination among technologies influence performance. Health and financial ecosystems face analogous challenges when institutions combine internal databases with external vendors, application programming interfaces, digital platforms, and cross-border services. Compliance controls must identify where data originate, which parties transform them, how interfaces are secured, and whether responsibility remains traceable when information crosses organizational or jurisdictional boundaries (Shittu et al., 2019).

Optimization technologies further illustrate the shift toward adaptive, data-driven control. Hybrid-energy research in developing economies highlights intelligent control, machine learning, and optimization for managing variable conditions. Similar techniques increasingly support health-risk prediction, fraud detection, transaction monitoring, resource allocation, and compliance prioritization. Their governance challenge lies in ensuring that improved predictive capability does not obscure model assumptions, introduce discriminatory outcomes, or weaken human accountability for consequential decisions (Sunday & Omoegun, 2019).

5.2 Regulatory Harmonization and Future Research

Regulatory harmonization is necessary because health and financial information now moves across institutions, platforms, jurisdictions, and professional domains whose legal requirements are not always compatible. Harmonization should not imply uniformity; rather, it should establish interoperable principles for lawful processing, verification, confidentiality, accountability, cross-border transfer, and supervisory cooperation. Comparative analysis of African privacy laws shows that national regimes have developed under overlapping international, continental, and regional influences, creating convergence but also differences in institutional design, enforcement, and implementation maturity (Greenleaf & Cottier, 2022).

The experience of regulatory cooperation in East Africa demonstrates that harmonized standards can strengthen capacity when they are supported by common guidelines, information-management systems, joint review mechanisms, quality systems, and institutional trust. Although developed for medical-products regulation, this experience offers a useful governance model for health-data compliance because effective harmonization depends on shared procedures and coordinated implementation rather than legal similarity alone (Ndomondo-Sigonda et al., 2021).

Cross-border digital activity also requires compatibility between privacy obligations and legitimate information exchange. European debates concerning the relationship between data protection and international trade illustrate how regulatory systems must preserve fundamental privacy safeguards while accommodating transnational data flows. Future frameworks for health and financial information should therefore define minimum protections, transfer conditions, accountability mechanisms, and mechanisms for resolving conflicting jurisdictional obligations (Yakovleva & Irion, 2020).

Harmonization ultimately depends on institutional capability. Nigerian evidence concerning professional attributes and organizational performance highlights the importance of competence, responsibility, communication, and professional effectiveness within complex organizations. Regulatory convergence will remain largely symbolic unless institutions possess personnel capable of interpreting shared standards, documenting compliance, managing exceptions, and coordinating with regulators and external partners (Onche, Adenekan & Sabboh, 2021).

Future research should consequently move beyond comparing statutes toward evaluating implementation quality, workforce readiness, technological interoperability, audit outcomes, enforcement consistency, and the effects of automated compliance systems. Workforce-centred operational research further demonstrates that performance depends on aligning tasks with human capability, variability, and organizational conditions rather than relying on static process assumptions (Akanbi, Ganiu & Sunday, 2022). Comparative studies should test whether harmonized verification rules reduce false matches, whether privacy controls preserve legitimate data access, and whether shared risk-screening standards improve consistency without creating exclusion or excessive surveillance. Priority should also be given to longitudinal research on regulatory technology, artificial intelligence, digital identity, cross-border cloud processing, and third-party accountability across health and financial ecosystems.

Conclusion

This review examined how information governance and regulatory compliance operate across health and financial systems, with particular attention to data verification, risk screening, confidentiality, identity management, access governance, breach response, digital transformation, and regulatory harmonization. The analysis fulfilled its central objective by demonstrating that both sectors rely on comparable governance principles, even though their operational contexts, legal mandates, and risk profiles differ. Across the evidence reviewed, data quality, integrity, provenance, and reliable verification emerged as foundational requirements for trustworthy decision-making, while risk-based monitoring and escalation were shown to be essential for identifying anomalies before they become material compliance failures.

The study further established that confidentiality cannot be protected through legal rules alone. Effective protection requires layered technical, organizational, and procedural controls, including authentication, role-based access, encryption, audit trails, incident response, and clearly assigned accountability. Comparative examination of health and financial systems also showed that identity verification and record validation must remain continuous processes, particularly where information is exchanged across institutions, platforms, and jurisdictions. At the same time, digital transformation is expanding the compliance perimeter through artificial intelligence, cloud services, distributed architectures, mobile platforms, and third-party processing, thereby increasing the need for adaptive governance.

Overall, the findings indicate that effective information governance depends on the integration of law, technology, institutional capacity, professional competence, and continuous oversight. Future policy should prioritize interoperable regulatory standards, stronger cross-border cooperation, transparent data-sharing rules, workforce development, and routine evaluation of automated compliance tools. Institutions should also adopt privacy-by-design, risk-based access models, tested breach-response procedures, and periodic validation of screening and verification systems. Future research should evaluate implementation outcomes across jurisdictions, particularly in emerging economies, and assess whether harmonized frameworks improve compliance consistency without undermining accessibility, innovation, or legitimate information exchange. These measures would strengthen accountability, resilience, public trust, and regulatory effectiveness across increasingly interconnected digital environments. Across both sectors over time globally.

References

1. Abdulkadir, A.B. and Sambo, A.O. (2022) ‘Data privacy rights and bankers’ business interests in Nigeria: Reflections on opportunities, challenges and legal reforms’, Jurnal Undang-undang dan Masyarakat, 30, pp. 3–16. DOI: 10.17576/juum-2022-30-01.
2. Adeniji, I.O., Shittu, H., Elumilade, R.A., Opara, I.S. and Shittu, M.A. (2020) ‘Grounding system design optimization for medium-voltage distribution networks in emerging power markets’, Iconic Research and Engineering Journals, 3(11), pp. 547–565. DOI: 10.64388/IREV3I11-1714040.
3. Agwuna, L., Irrshad, K. and Mazorodze, B.T. (2022) ‘Assessing monetary policy via the Taylor Rule in a selection of middle-income emerging market economies: Issues and evidence’, Management and Economics Research Journal, 8(2), pp. 1–14. DOI: 10.18639/MERJ.2022.9900060.

4. Akanbi, O., Ganiu, O.S. and Sunday, E.A. (2022) 'A workforce-centric line balancing model for throughput maximization in multi-shift operations', Shodhshauryam: International Scientific Refereed Research Journal, 5(3), pp. 439–464. DOI: 10.32628/SHISRRJ.
5. Akanbi, O., Ganiu, O.S. and Sunday, E.A. (2022) 'Comprehensive review of statistical process control (SPC) for precision weight management in global food manufacturing', Gyanshauryam: International Scientific Refereed Research Journal, 5(3), pp. 433–461. Available at: https://gisrrj.com/paper/GISRRJ225387.pdf.
6. Akin-Oluyomi, O.T. and Akhigbe, R. (2022) 'A supply chain governance model for enhancing compliance and operational quality across retail networks', International Journal of Multidisciplinary Research and Growth Evaluation, 3(6), pp. 860–878. DOI: 10.54660/.IJMRGE.2022.3.6.860-878.
7. Arasa, R. and Ottichilo, L. (2015) 'Determinants of Know Your Customer (KYC) compliance among commercial banks in Kenya', Journal of Economics and Behavioral Studies, 7(2), pp. 162–175. DOI: 10.22610/jebs.v7i2(J).574.
8. Arner, D.W., Zetzsche, D.A., Buckley, R.P. and Barberis, J.N. (2019) 'The identity challenge in finance: From analogue identity to digitized identification to digital KYC utilities', European Business Organization Law Review, 20(1), pp. 55–80. DOI: 10.1007/s40804-019-00135-1.
9. Asrow, K. (2022) 'Defining data rights and the role of the individual', in Jeng, L. (ed.) Open Banking. Oxford: Oxford University Press, pp. 31–54. DOI: 10.1093/oso/9780197582879.003.0003.
10. Babalola, O. (2022) 'Nigeria's data protection legal and institutional model: an overview', International Data Privacy Law, 12(1), pp. 44–52. DOI: 10.1093/idpl/ipab023. (OUP Academic)
11. Ball, K., Canhoto, A., Daniel, E., Dibb, S., Meadows, M. and Spiller, K. (2020) 'Organizational tensions arising from mandatory data exchange between the private and public sector: The case of financial services', Technological Forecasting and Social Change, 155, 119996. DOI: 10.1016/j.techfore.2020.119996.
12. Balogun, C.T. and Sabboh, G.M. (2021) 'Psycho-sociological factors as determinants of juvenile delinquency among adolescents in junior secondary schools in Patani Local Government Area of Delta State, Nigeria', International Journal of Academic Management Science Research, 5(10), pp. 34–40.
13. Botchey, F.E., Qin, Z. and Hughes-Lartey, K. (2020) 'Mobile money fraud prediction—A cross-case analysis on the efficiency of support vector machines, gradient boosted decision trees, and Naïve Bayes algorithms', Information, 11(8), 383. DOI: 10.3390/info11080383.
14. Chen, H., Yu, P., Hailey, D. and Cui, T. (2020) 'Identification of the essential components of quality in the data collection process for public health information systems', Health Informatics Journal, 26(1), pp. 664–682. DOI: 10.1177/1460458219848622.
15. Dove, E.S. and Chen, J. (2020) 'Should consent for data processing be privileged in health research? A comparative legal analysis', International Data Privacy Law, 10(2), pp. 117–131. DOI: 10.1093/idpl/ipz023.
16. Ejofodomi, O.A., Gideon, E.N., Oladipo, G.O. and Oshomah, E.R. (2014) 'Automated detection of architectural features in mammograms using template matching', International Journal of Biomedical Science and Engineering, 2(1), pp. 1–6. DOI: 10.11648/j.ijbse.20140201.11.

17. Ekong, I., Chukwu, E. and Chukwu, M. (2020) 'COVID-19 mobile positioning data contact tracing and patient privacy regulations: Exploratory search of global response strategies and the use of digital tools in Nigeria', JMIR mHealth and uHealth, 8(4), e19139. DOI: 10.2196/19139.
18. Enaifoghe, A., Dlamini, N.P. and Agwuna, L.U. (2020) 'African economic integration development in technological transformation: Assessing the importance of ethical leadership for policy implementation in SADC', Journal of Economics and Behavioral Studies, 12(6), pp. 11–20. DOI: 10.22610/jebs.v12i6(J).3102.
19. Ezeani, P.T. and Sabboh, G.M. (2021) 'Psychosocial predictors of the changing role of husbands as breadwinners in a depressed economy in Ibadan Metropolis, Oyo State, Nigeria', British Journal of Education, Learning and Development Psychology, 4(2), pp. 31–42. DOI: 10.52589/BJELDP-ZU3KSUJU.
20. Fadahunsi, K.P., O'Connor, S., Akinlua, J.T., Wark, P.A., Gallagher, J., Carroll, C., Car, J., Majeed, A. and O'Donoghue, J. (2021) 'Information quality frameworks for digital health technologies: Systematic review', Journal of Medical Internet Research, 23(5), e23479. DOI: 10.2196/23479.
21. Falemi, A., Akhigbe, R. and Akin-Oluyomi, O.T. (2020) 'A conceptual supply chain talent development model for capability building across distributed operations', International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), pp. 439–456. DOI: 10.54660/.IJMRGE.2020.1.5.439-456.
22. Gatchalian, N., Kandy, M.C. and Sattler, D.M. (2022) 'Protecting privacy of health information, a global perspective', Studies in Health Technology and Informatics, 290, pp. 230–233. DOI: 10.3233/SHTI220068.
23. Greenleaf, G. and Cottier, B. (2022) 'International and regional commitments in African data privacy laws: A comparative analysis', Computer Law & Security Review, 44, 105638. DOI: 10.1016/j.clsr.2021.105638.
24. Guckert, M., Milanovic, K., Hannig, J., Simon, D., Wettengl, T., Evers, D., Kleyer, A., Keller, T. and Pitt, J. (2022) 'The disruption of trust in the digital transformation leading to Health 4.0', Frontiers in Digital Health, 4, 815573. DOI: 10.3389/fdgth.2022.815573.
25. Haeri Mazanderani, A., Sherman, G.G., Moyo, F., Goga, A.E. and Feucht, U. (2018) 'Leveraging the Road to Health booklet as a unique patient identifier to monitor the prevention of mother-to-child transmission programme', South African Medical Journal, 108(9), pp. 729–733. DOI: 10.7196/SAMJ.2018.v108i9.13093.
26. Henning, J. and Hauman, M. (2017) 'Fortifying a risk-based approach in the South African AML/CFT process', Journal of Financial Crime, 24(4), pp. 520–528. DOI: 10.1108/JFC-01-2017-0007.
27. Hilal, W., Gadsden, S.A. and Yawney, J. (2022) 'Financial fraud: A review of anomaly detection techniques and recent advances', Expert Systems with Applications, 193, 116429. DOI: 10.1016/j.eswa.2021.116429.
28. Holst, C., Sukums, F., Radovanovic, D., Ngowi, B., Noll, J. and Winkler, A.S. (2020) 'Sub-Saharan Africa—the new breeding ground for global digital health', The Lancet Digital Health, 2(4), pp. e160–e162. DOI: 10.1016/S2589-7500(20)30027-3.
29. Ikwegbue, P.C., Enaifoghe, A.O., Maduku, H. and Agwuna, L.U. (2021) 'The challenges of COVID-19 pandemic and South Africa's response', African Renaissance, 18(1), pp. 271–292. DOI: 10.31920/2516-5305/2021/18n1a13.

30. Jalali, M.S., Russell, B., Razak, S. and Gordon, W.J. (2019) 'EARS to cyber incidents in health care', Journal of the American Medical Informatics Association, 26(1), pp. 81–90. DOI: 10.1093/jamia/ocy148.
31. Javed, I.T., Alharbi, F., Bellaj, B., Margaria, T., Crespi, N. and Qureshi, K.N. (2021) 'Health-ID: A blockchain-based decentralized identity management for remote healthcare', Healthcare, 9(6), 712. DOI: 10.3390/healthcare9060712.
32. Keshta, I. and Odeh, A. (2021) 'Security and privacy of electronic health records: Concerns and challenges', Egyptian Informatics Journal, 22(2), pp. 177–183. DOI: 10.1016/j.eij.2020.07.003. (DOI)
33. Maïga, A., Jiwani, S.S., Mutua, M.K., Porth, T.A., Taylor, C.M., Asiki, G., Melesse, D.Y., Day, C., Strong, K.L., Faye, C.M., Viswanathan, K., O'Neill, K.P., Amouzou, A., Pond, B.S. and Boerma, T. (2019) 'Generating statistics from health facility data: The state of routine health information systems in Eastern and Southern Africa', BMJ Global Health, 4(5), e001849. DOI: 10.1136/bmjgh-2019-001849.
34. Marelli, L., Lievevrouw, E. and Van Hoyweghen, I. (2020) 'Fit for purpose? The GDPR and the governance of European digital health', Policy Studies, 41(5), pp. 447–467. DOI: 10.1080/01442872.2020.1724929.
35. Meribole, E.C., Makinde, O.A., Oyemakinde, A., Oyediran, K.A., Atobatele, A., Fadeyibi, F.A., Azeez, A., Ogbokor, D., Adebayo, O., Adebayo, W., Abatta, E., Adoghe, A., Adebayo, S.B., Mahmoud, Z., Ashefor, G., Adebayo, S.B., Yisa, I.O., Balogun, A., Chukwujekwu, O., Dalhatu, I., Jahun, I., Bamidele, S., Johnson, D.O., Ibrahim, M., Akpan, F., Aiyenigba, B., Omaha, O.I., Terpase, A., Ottih, C., Adelakin, O., Mullen, S. and Orobaton, N. (2018) 'The Nigerian health information system policy review of 2014: The need, content, expectations and progress', Health Information & Libraries Journal, 35(4), pp. 285–297. DOI: 10.1111/hir.12240.
36. Meyer, G.D., Meyer, N., Du Toit, J.D., Mans, P.A. and Moffett, B.D. (2021) 'WhatsApp-appropriate? A retrospective content analysis of WhatsApp use and potential breaches in confidentiality among a team of doctors at a district hospital, South Africa', South African Medical Journal, 111(2), pp. 171–175. DOI: 10.7196/SAMJ.2021.v111i2.14453.
37. Mizrahi-Borohovich, I. and Levi-Faur, D. (2020) 'Varieties of consumer credit data regimes: A regulatory governance approach', Governance, 33(1), pp. 109–134. DOI: 10.1111/gove.12473. (Wiley Online Library)
38. Ndomondo-Sigonda, M., Miot, J., Naidoo, S., Masota, N.E., Ng'andu, B., Ngum, N. and Kaale, E. (2021) 'Harmonization of medical products regulation: A key factor for improving regulatory capacity in the East African Community', BMC Public Health, 21, 187. DOI: 10.1186/s12889-021-10169-1.
39. OECD (2022) Health Data Governance for the Digital Age: Implementing the OECD Recommendation on Health Data Governance. Paris: OECD Publishing. DOI: 10.1787/68b60796-en.
40. Olutimehin, A.O. and Ganiu, O.S. (2022) 'Integrating Lean Six Sigma with reliability-centered maintenance: A unified framework for manufacturing excellence', International Journal of Multidisciplinary Research and Growth Evaluation, 3(6), pp. 983–996. DOI: 10.54660/.IJMRGE.2022.3.6.983-996.

41. Onche, V.O., Adenekan, E.T. and Sabboh, G.M. (2021) 'Influence of personal and professional attributes of secretaries on organisational success of universities in Oyo State, Nigeria', International Journal of Science Academic Research, 2(4), pp. 1355–1359.
42. Oyarekua, T.A. and Sabboh, G.M. (2021) 'Parenting styles and effortful control as predictors of mental health among secondary school adolescents in Akinyele Local Government Area, Oyo State, Nigeria', International Journal of Academic Multidisciplinary Research, 5(10), pp. 108–114.
43. Padmanabhan, S., Carty, L., Cameron, E., Ghosh, R.E., Williams, R. and Strongman, H. (2019) 'Approach to record linkage of primary care data from Clinical Practice Research Datalink to other health-related patient data: Overview and implications', European Journal of Epidemiology, 34, pp. 91–99. DOI: 10.1007/s10654-018-0442-4.
44. Parra Moyano, J. and Ross, O. (2017) 'KYC optimization using distributed ledger technology', Business & Information Systems Engineering, 59(6), pp. 411–423. DOI: 10.1007/s12599-017-0504-2.
45. Rockwern, B., Johnson, D. and Snyder Sulmasy, L. (2021) 'Health information privacy, protection, and use in the expanding digital health ecosystem: A position paper of the American College of Physicians', Annals of Internal Medicine, 174(7), pp. 994–998. DOI: 10.7326/M20-7639.
46. Sabboh, G.M. (2021) 'Psychosocial factors as predictors of moral disengagement among in-school adolescents in Ibadan Metropolis', International Journal of Academic Information Systems Research, 5(10), pp. 1–7.
47. Sabboh, G.M. (2022) Development and validation of the revised self-esteem scale for Nigerian adolescents and youths. Master's thesis. Moscow, Russia: National Research University Higher School of Economics.
48. Sabboh, G.M. and Alausa, S.S. (2021) 'School climate, self-efficacy, social media and peer pressure as correlates of aggressive behaviour among secondary school adolescents in Ibadan Metropolis, Oyo State, Nigeria', International Journal of Academic Management Science Research, 5(11), pp. 43–51.
49. Sabboh, G.M. and Olugbade, D. (2021) 'Influence of teaching styles and parental bonding on academic boredom among undergraduates in Oyo State, Nigeria', African Journal of Social Sciences and Humanities Research, 4(1), pp. 122–133.
50. Sabboh, G.M. and Yusuf, A.O. (2021) 'Influence of psycho-social factors as predictors of child abuse among junior secondary school students in Kaduna Metropolis of Kaduna State', International Journal of Academic and Applied Research, 5(8), pp. 18–24.
51. Scheibner, J., Ienca, M., Kechagia, S., Troncoso-Pastoriza, J.R., Raisaro, J.L., Hubaux, J.P., Fellay, J. and Vayena, E. (2020) 'Data protection and ethics requirements for multisite research with health data: A comparative examination of legislative governance frameworks and the role of data protection technologies', Journal of Law and the Biosciences, 7(1), lsaa010. DOI: 10.1093/jlb/lsaa010.
52. Schlatt, V., Sedlmeir, J., Feulner, S. and Urbach, N. (2022) 'Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity', Information & Management, 59(7), 103553. DOI: 10.1016/j.im.2021.103553.
53. Semantha, F.H., Azam, S., Yeo, K.C. and Shanmugam, B. (2020) 'A systematic literature review on privacy by design in the healthcare sector', Electronics, 9(3), 452. DOI: 10.3390/electronics9030452.

54. Shi, M., Jiang, R., Hu, X. and Shang, J. (2020) 'A privacy protection method for health care big data management based on risk access control', Health Care Management Science, 23(3), pp. 427–442. DOI: 10.1007/s10729-019-09490-4.
55. Shittu, H., Opara, I.S., Elumilade, R.A., Liadi, K.O. and Adeniji, I.O. (2019) 'Hydrogen as a secondary energy carrier: Modeling its integration in national grids', Iconic Research and Engineering Journals, 3(1), pp. 628–643. DOI: 10.64388/IREV3I1-1713909.
56. Shittu, H.A., Shittu, M.A., Adeleke, O.J. and Adedokun, O.J. (2021) 'Blockchain-based energy trading models for peer-to-peer renewable microgrids', International Journal of Research in Electrical and Electronics Engineering, 4(3), pp. 1–19. DOI: 10.34218/IJREEE_04_03_001.
57. Shittu, M.A., Adeniji, I.O., Shittu, H. and Opara, I.S. (2022) 'Blockchain-assisted secure data exchange architectures for SCADA-controlled power systems', Iconic Research and Engineering Journals, 6(3), pp. 359–380. DOI: 10.64388/IREV6I3-1714041.
58. Simon, M. and Looten, V. (2020) 'Description of data breaches notifications in France and lessons learned for the healthcare stakeholders', Studies in Health Technology and Informatics, 275, pp. 192–196. DOI: 10.3233/SHTI200721.
59. Staunton, C., Tschigg, K. and Sherman, G. (2021) 'Data protection, data management, and data sharing: Stakeholder perspectives on the protection of personal health information in South Africa', PLOS ONE, 16(12), e0260341. DOI: 10.1371/journal.pone.0260341.
60. Sunday, E.A. and Omoegun, G.O. (2018) 'Integrating solar power solutions in small-scale manufacturing industries in Nigeria', International Journal of Scientific Research in Science, Engineering and Technology, 4(8), pp. 832–853.
61. Sunday, E.A. and Omoegun, G.O. (2019) 'Optimizing electrical load distribution for hybrid solar installations in developing economies', International Journal of Scientific Research in Mechanical and Materials Engineering, 3(6), pp. 27–47.
62. Sunday, E.A. and Omoegun, G.O. (2020) 'Smart fault detection in HVAC systems using sensor-based monitoring', International Journal of Scientific Research in Science, Engineering and Technology, 7(4), pp. 380–403.
63. Sunday, E.A. and Omoegun, G.O. (2022) 'Automation of process control systems using Siemens TIA Portal: A case study approach', International Journal of Scientific Research in Mechanical and Materials Engineering, 6(5), pp. 30–55.
64. Sunday, E.A., Omoegun, G.O., Essien, M.A. and Oluokun, O.A. (2019) 'Thermodynamic efficiency and control strategies in residential air conditioning systems', International Journal of Scientific Research in Civil Engineering, 3(3), pp. 52–76. DOI: 10.32628/IJSRCE19339.
65. Sunday, E.A., Omoegun, G.O., Essien, M.A. and Oluokun, O.A. (2020) 'Transitioning from reactive to predictive maintenance in mechanical systems', International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 6(6), pp. 425–447.
66. Swales, L. (2022) 'The Protection of Personal Information Act 4 of 2013 in the context of health research: Enabler of privacy rights or roadblock?', Potchefstroom Electronic Law Journal, 25, pp. 1–32. DOI: 10.17159/1727-3781/2022/v25i0a11180.
67. Turki, M., Hamdan, A., Cummings, R.T., Sarea, A., Karolak, M. and Anasweh, M. (2020) 'The regulatory technology "RegTech" and money laundering prevention in Islamic and

conventional banking industry', Heliyon, 6(10), e04949. DOI: 10.1016/j.heliyon.2020.e04949.

68. Vo, K., Jonnagaddala, J. and Liaw, S.T. (2019) 'Statistical supervised meta-ensemble algorithm for medical record linkage', Journal of Biomedical Informatics, 95, 103220. DOI: 10.1016/j.jbi.2019.103220.
69. von Solms, J. (2021) 'Integrating Regulatory Technology (RegTech) into the digital transformation of a bank Treasury', Journal of Banking Regulation, 22(3), pp. 191–207. DOI: 10.1057/s41261-020-00138-w.
70. Warikandwa, T.V. (2021) 'Personal data security in South Africa's financial services market: The Protection of Personal Information Act 4 of 2013 and the European Union General Data Protection Regulation compared', Potchefstroom Electronic Law Journal, 24, pp. 1–32. DOI: 10.17159/1727-3781/2021/v24i0a10727. (Potchefstroom Electronic Law Journal)
71. Weiskopf, N.G. and Weng, C. (2013) 'Methods and dimensions of electronic health record data quality assessment: Enabling reuse for clinical research', Journal of the American Medical Informatics Association, 20(1), pp. 144–151. DOI: 10.1136/amiajnl-2011-000681.
72. Winter, J.S. and Davidson, E. (2022) 'Harmonizing regulatory regimes for the governance of patient-generated health data', Telecommunications Policy, 46(5), 102285. DOI: 10.1016/j.telpol.2021.102285.
73. Yakovleva, S. and Irion, K. (2020) 'Toward compatibility of the EU trade policy with the General Data Protection Regulation', AJIL Unbound, 114, pp. 10–14. DOI: 10.1017/aju.2019.81.
74. Yusuf, A.O. and Sabboh, G.M. (2021) 'Psychological factors as correlates of suicidal ideation among university students in Lagos State', International Journal of Academic and Applied Research, 5(9), pp. 1–7.