

Table S2. Characteristics of Included Studies

Title (Author /Institution, Year)	Study or Document focus/goal	Summary of findings		
		Governance and institutional authority	Interoperability Arrangements and System Integration	¹ Regulatory Gaps and Enforcement Constraints
Peer-reviewed published articles				
Transitioning to digital transactional data capture in primary health care facilities: a case report from Ghana’s Savannah Region (Abotsi et al., 2025)	Examine the implementation of digital transactional data capture for maternal and child health services in Ghana’s Savannah Region and identify enablers and barriers to uptake in resource-limited settings.	• Governance is led by Ghana Health Service (GHS) with oversight from PPMED/CHIM, and subnational leadership at regional and district levels. • The study finds that weak subnational governance, limited leadership ownership, and inadequate decentralized technical support undermined sustained adoption. • Strong facility and district leadership, supervision, and ownership were critical enablers where adoption was sustained.	• e-Tracker is implemented as a DHIS2 Tracker module, operating in parallel with paper-based systems and feeding aggregate reporting into DHIMS2. • The study highlights lack of seamless integration between transactional systems (e-Tracker) and aggregate or EMR systems. • No bi-directional interoperability framework is operational; data synchronization depends on connectivity and system configuration completeness.	• Mandatory parallel use of paper and electronic systems, described as a government directive • Absence of clear policy direction to transition to paperless systems • Weak enforcement of transition timelines constrained full electronic adoption. • Lack of decentralized governance and technical authority at subnational levels
Mapping the regulatory landscape of AI in healthcare in Africa	Map the existing regulatory instruments relevant to artificial	• Finds no sui generis AI governance frameworks in	• No formal AI-specific interoperability frameworks identified.	• Absence of AI-specific legislation or binding regulatory guidance

¹ Regulatory gaps are reported only where explicitly identified or framed as legal, policy, or enforcement constraints in the source documents. Operational, technical, or organizational challenges are not classified as regulatory gaps unless stated by the source

(Townsend et al., 2023)	intelligence in healthcare and health research across 12 African countries, including Ghana.	any of the 12 countries studied. • Governance of AI in healthcare is indirect and fragmented, relying on existing authorities in health, data protection, ICT, consumer protection, and medical devices, with weak coordination between regulators. • No dedicated AI oversight bodies exist for healthcare.	• Interoperability relevant to AI is indirectly supported through digital health policies, data protection laws, and regional data-sharing initiatives (e.g. AU Data Policy Framework, sub-regional health data-sharing frameworks). These are not operational AI interoperability architectures.	• Fragmented and sector-specific regulatory instruments not designed for AI • Lack of clear rules for AI as software-as-a-medical-device • Insufficient regulatory guidance on data governance, validation, accountability, and lifecycle oversight of AI systems • Weak harmonization across countries • Limited regulatory capacity to govern AI deployment in healthcare.
Maternal and child health data quality in health care facilities at the Cape Coast Metropolis, Ghana (Lasim et al., 2022)	Assess the level of maternal and child health (MCH) data quality in health care facilities in the Cape Coast Metropolis using the dimensions of accuracy, completeness, timeliness, and consistency.	• Data governance is exercised through Ghana Health Service (GHS) routine health information management structures, including facility heads, validation teams, and district oversight. • The study evidences active data validation and reporting accountability mechanisms within DHIS2, though variability exists across facility types, particularly CHPS compounds and private facilities.	• DHIS2 functions as the national health data repository, receiving data from paper-based registers and standardized monthly reporting forms. • The study evaluates data transfer and consistency across registers, forms, and DHIS2, but does not describe or propose new interoperability architectures or frameworks beyond existing DHIS2 workflows.	Not identified in source
Ethics and Electronic Health Information Technology: Challenges for Evidence-Based	Explore national legislation on Electronic Health	• Governance of electronic health information is found to be fragmented and weak,	• Interoperability is discussed conceptually as the automatic exchange of	• Absence of national legislation regulating capture, storage, primary

Medicine and the Physician–Patient Relationship (Norman et al., 2011)	Information Technology, ethical implications of EHIT, and effects on the physician–patient relationship in Ghana.	spread across NHIS, NIA, GHS, and other public institutions without a coordinating authority. • Oversight of access, secondary use, and accountability for electronic health data is unclear. • Ethical governance mechanisms for EHIT are underdeveloped, leaving professional ethics as the primary safeguard.	patient data across NHIS, NIA, and other national databases. • The paper does not propose a technical interoperability framework but highlights that increasing interoperability without safeguards amplifies risks to confidentiality, trust, and professional autonomy.	and secondary use of electronic health records • Lack of privacy law governing health data; NHIS regulations silent on privacy • No regulation governing access, auditing, or secondary use of health records • No legal standards protecting physician–patient confidentiality in an interoperable digital environment.
A review of the Ghana National Health Insurance Scheme claims database: possibilities and limits for drug utilization research (Ankrah et al., 2019)	Describe the content, structure, coverage, possibilities, and limitations of the NHIS claims database for drug utilization research in Ghana.	• Governance of the NHIS claims database is exercised by the National Health Insurance Authority (NHIA) under the National Health Insurance Act. • The paper documents formal governance mechanisms for claims submission, vetting, adjudication, reimbursement, and fraud control, with standardized accreditation, provider codes, client identifiers, and multi-stage review workflows.	The claims database uses standardized coding systems including ICD-10, G-DRG, ATC, and NHIS medicine codes. The authors explicitly note that the database can be transformed into existing Common Data Models (e.g. FDA Sentinel CDM) to enable interoperability and cross-country comparison, but no national health-sector interoperability framework linking NHIS to other systems is operational.	• Absence of a common national patient identifier across public and private insurers, limiting linkage of NHIS data with private insurance databases • Lack of legal and institutional arrangements for routine cross-database linkage; and absence of policy mechanisms to mandate harmonized identifiers across insurance schemes. • Other limitations (partial electronic claims coverage, missing OTC and vertical-programme medicines) are reported as system constraints, not policy barriers.

Framework on mobile technology utilization for assisted healthcare service request and delivery for aged persons: a case of Ghana (Agbehadji et al., 2019)	Develop a conceptual framework to guide the utilization of mobile technology for assisted healthcare service request and delivery for aged persons in Ghana, while creating employment opportunities for graduate health professionals.	• Governance is described at a conceptual level, involving verification of professional credentials, role definition for health professionals, hospitals, and patients, and assignment of responsibilities within the proposed mHealth platform. • No national or sector-wide governance mechanisms are evaluated or empirically assessed.	• Proposes a conceptual interoperability design using mobile phones, middleware, and event-based data flow to control information exchange across domains (patients, health professionals, payment platforms). • Interoperability is discussed as controlled data exchange with policy enforcement at middleware level, but no alignment with national interoperability frameworks or standards is specified.	Not identified in the source
Implementation of Electronic Health Record System in Ghana: A Review (Achampong, 2022)	Assess why, despite implementation of electronic health record systems in Ghana, there has been no significant improvement in patient outcomes, with emphasis on implementation challenges.	• Finds weak governance and leadership in EHR implementation. • Implementation was predominantly top-down, led by MoH and GHS, with limited end-user involvement. • Lack of facility-level leadership ownership, absence of champions, inadequate organizational alignment, and weak accountability mechanisms undermined sustained use.	• Reports absence of national EHR interoperability guidelines at the time of implementation. • Public hospitals procured disparate EHR systems that could not interoperate with each other or with NHIS claims systems. • Software interoperability failures, lack of system integration with reporting workflows, and absence of standards for cross-facility data exchange were major constraints.	• Lack of policy support and absence of clear national guidelines for EHR implementation • No mandated interoperability standards; insufficient policy direction on end-user engagement, workflow integration, and reporting automation • Absence of policy mechanisms to align infrastructure readiness with EHR rollout.

Compliance with Electronic Medical Records Privacy Policy: A Perspective of Employees of a Private Hospital in Accra, Ghana (Wallace-bruce, 2021)	Investigate factors affecting employee compliance with electronic medical records (EMR) privacy policies at Nyaho Medical Centre.	• Governance of EMR privacy is exercised at the institutional level through hospital management, the Medical Director, and internal policies aligned with the Data Protection Act, 2012 (Act 843). • Staff are required to sign confidentiality clauses and non-disclosure agreements. • The study finds high awareness and high compliance, supported by sanctions, supervision, and internal enforcement rather than national digital health governance mechanisms.	Interoperability is not a focus of the study. EMR use is described as facility-specific, with no discussion of interoperability with national systems (DHIMS2, NHIS, or other hospitals) or use of interoperability standards or frameworks.	Not identified in source
Evaluating the impact of Electronic Health Records on Healthcare Quality in Resource-Limited Settings: Evidence from a Ghanaian Mission Hospital (Ofori, 2025)	Examine the impact of Electronic Health Records on the quality of healthcare delivery at Our Lady of Grace Hospital in a resource-limited setting in Ghana.	• Governance of the EHR system is exercised at the facility level through hospital management and departmental supervision. • EHR use is mandatory across departments, with operational oversight by administrators, clinicians, and IT staff. • Governance is primarily organizational and managerial, with no analysis of national digital health governance structures or regulatory oversight.	• The EHR system operates as an internal, facility-based system supporting simultaneous multi-departmental access to patient records. • The study describes shared access and real-time use across departments but does not reference national interoperability frameworks, standards, or integration with DHIMS2, NHIS, or other external systems.	Not identified in the source.

mHealth and digital innovations as catalysts for transforming mental health care in Ghana (Sackey et al., 2024)	Examine how mHealth and digital innovations can address systemic gaps in Ghana's mental health care delivery and outline strategic actions to accelerate their adoption and integration.	• Governance of mental health and digital innovations is described as fragmented, spanning the Ministry of Health, Mental Health Authority, Ghana Health Service, and informal actors (traditional and faith healers), with weak coordination and underfunded implementation of the Mental Health Act, 2012. • Digital mental health initiatives are largely project-driven, with limited institutionalisation and reliance on partnerships such as WADMA.	Interoperability is discussed at a conceptual and strategic level. The authors call for integration of digital mental health tools into hospital systems and alignment with national EHR and telemedicine initiatives, but do not specify technical standards, architectures, or operational interoperability frameworks.	• Underfunding and slow implementation of the Mental Health Act, 2012 • Insufficient NHIS coverage for mental health services; lack of institutionalized digital mental health training • Absence of national mechanisms to scale digital mental health pilots • Weak integration of digital tools into formal health system workflows.
Grey Literature Sources				
Ghana e-Health Strategy (Ministry of Health, 2010)	The goal of the e-health strategy is to harness the potential of Information and Communication Technology to improve the health status of people living in Ghana.	• No operational national e-health governance structure existed at baseline. • Governance weaknesses included fragmented ownership of ICT initiatives, lack of coordination across MoH agencies, absence of accountability mechanisms, and no formal oversight of e-health investments. • The strategy proposes establishment of a Ministerial Committee on	• No operational e-health architecture at baseline. Existing systems were siloed, used different operating systems and data sets, and could not exchange data. • The strategy proposes a National E-Health Architecture, alignment with the e-Government Interoperability Framework, adoption of international standards (e.g. ICD, HL7, DICOM),	• No health-sector regulatory framework for electronic data exchange, privacy, security, or consent. • Ownership of electronic health data undefined. • Weak enforcement of ICT policies. Fragmented provider landscape complicating standardization. • Chronic underinvestment in ICT infrastructure.

		E-Health, chaired by political leadership, supported by an interagency technical structure to review, approve, align, and monitor all e-health initiatives and standards.	development of unique patient and facility identifiers, harmonized data standards, and integration of existing systems including DHIMS and NHIS platforms.	• Dependence on donor-funded pilots with sustainability risks. • Limited ICT human resource capacity and absence of a formal scheme of service.
Health Information Systems Strategic Plan (HISSP) (Ministry of Health Ghana, 2022)	To institutionalize an integrated health information system that ensures availability of quality health data for decision making at all levels.	• Governance of the health information system is led by the Minister for Health through the Inter-Agency Leadership Committee (IALC), with coordination by the Policy, Planning, Monitoring and Evaluation Directorate (PPME) and technical oversight by Research, Statistics and Information Management (RSIM) and the Information, Monitoring and Evaluation Technical Working Group (IME-TWG). CHIM manages DHIMS2 but faces authority and coordination challenges across MoH agencies. • Existing governance arrangements are acknowledged as weak, fragmented, and not fully functional, particularly the IME-TWG.	• Absence of interoperability standards at baseline. The plan proposes development of sector-wide interoperability standards, harmonization of data capture tools, integration of fragmented systems, expansion of DHIMS2 as the national data repository, creation of interfaces between agency systems and DHIMS2, and alignment with NITA national interoperability standards.	• Lack of a National Health Information System Policy • Weak enforcement of existing standards • Fragmented and duplicative information systems; limited interoperability across agencies; inadequate financing • Dependence on development partners; insufficient ICT and human resource capacity • Weak coordination across MoH agencies • Resistance to data sharing • Inconsistent data structures • Absence of formal data-sharing agreements.

Ghana eGovernment Interoperability Framework (eGIF) Version 2.0 (Government of Ghana, 2014)	To promote and support the delivery of Government of Ghana Digital Services by fostering cross-sectoral interoperability.	• eGIF is governed as a Government of Ghana asset under the Government of Ghana Enterprise Architecture (GGEA) programme. • NITA acts as the owner, responsible for day-to-day management and maintenance, supported by a GGEA/eGIF Working Group drawn from MDAs. • Compliance with eGIF standards is to be enforced through architecture compliance reviews, tied to project approval and funding decisions.	• Defines a comprehensive whole-of-government interoperability framework covering legal, organisational, semantic, and technical interoperability. • Introduces a Digital Services Conceptual Model built on service-oriented architecture, Enterprise Service Bus (ESB), APIs, secure data exchange, base registries, and aggregated services. • Specifies detailed interoperability standards across channels, business processes, data, networks, security, applications, and SOA, with mandatory use of agreed standards and interoperability agreements (MoUs, SLAs).	• Fragmented legacy systems acquired on a solution-by-solution basis • Weak implementation of earlier eGIF and GGEA (2008) iterations • Lack of harmonized legal frameworks across MDAs • Inconsistent enforcement of standards; organizational resistance to data sharing • Capacity gaps within MDAs • High coordination burden for cross-agency collaboration.
Data Protection Act, 2012 (Act 843) (Parliament of Ghana, 2012)	To establish a Data Protection Commission, to protect the privacy of the individual and personal data by regulating the processing of personal information, and to provide the process to obtain, hold, use	• Establishes the Data Protection Commission (DPC) with a governing Board appointed by the President. The Commission has statutory authority to regulate, monitor compliance, investigate complaints, maintain a Data Protection Register,	• The Act does not define technical interoperability standards. • It provides legal interoperability conditions for data exchange through mandatory principles governing data processing, consent, purpose limitation, security safeguards, breach	• Absence of sector-specific operational guidance, including for health data. Broad ministerial exemption powers (e.g. national security, public interest). • Limited specification of enforcement mechanisms beyond registration and penalties.

	or disclose personal information.	issue enforcement notices, and impose sanctions. • All government departments are defined as data controllers and required to designate data supervisors. • Minister retains power to issue policy directives to the Commission.	notification, registration of data controllers, and lawful cross-border data processing. • Interoperability is permitted only where processing complies with these statutory conditions.	• No explicit alignment mechanisms with sectoral digital systems or interoperability frameworks. • Compliance burden for public institutions without corresponding technical or financial support mechanisms.
Policy and Strategy on Digital Health (2023–2027) (Ghana Health Service, 2023)	Contribute to increasing access to comprehensive and quality health services through the use of ICT by 2027.	• Governance responsibility rests with Ghana Health Service under the Director-General, supported by a National Digital Health Steering Committee, Digital Health Technical Working Group, and Regional Digital Health Technical Committees. • The policy explicitly targets weaknesses in leadership, accountability, coordination, and oversight of digital health initiatives across national, regional, district, and sub-district levels. • Strengthening governance and accountability is identified as a primary strategic objective.	• Interoperability is defined as a guiding principle and a standalone strategic objective. • The policy commits to open standards, open source, and development of an integrated health enterprise architecture. • It calls for interoperable digital solutions, seamless and secure data exchange across systems, reduction of siloed applications, alignment with national interoperability frameworks, and establishment of an integrated information architecture to enable cross-system data sharing within GHS.	• Fragmented and non-interoperable digital systems • Absence of harmonized digital health standards • Weak policy and regulatory enforcement • Parallel ICT investments • Inadequate ICT infrastructure • Obsolete networks, limited funding • Over-reliance on donor support • Insufficient skilled ICT personnel • Cybersecurity risks, and resistance to system integration across units.
Ghana Health Data Ecosystem Mapping: Scaling the Use of Digital Tools for Vaccination	Provide an overview of current digital immunization systems used in	• Finds that GHS has established digital health governance mechanisms, including the Digital Health	• Identifies lack of interoperability as the dominant system-wide gap.	• Non-integrated and siloed digital systems • Absence of a functional interoperability layer;

Planning, Deployment and Monitoring (GIZ, 2023)	Ghana and outline priorities so that Ghana – led by the direction of GHS and its existing governance mechanisms can develop and operationalize interoperable digital systems that support immunization from end to end.	Technical Working Group (DHTWG), Regional Digital Health Technical Committees (RDHTCs), and a National Digital Health Steering Committee, which oversee digital health initiatives and implementation of the national digital health strategy. • Governance structures exist but coordination across systems and stakeholders remains a challenge due to rapid, parallel system growth.	• Recommends establishment of an interoperability layer aligned with OpenHIE architecture and use of HL7 FHIR standards to enable secure data exchange between priority systems (DHIMS2, e-Tracker, SORMAS, GhiLMIS, LHIMS). • Proposes defining and validating data exchange requirements and piloting interoperability between two to three systems.	unreliable internet connectivity • Lack of funding for server infrastructure and data connectivity • Dependence on donor-funded systems • Gaps in core digital immunization components (digital certificates, microplanning tools, master facility registry, national product catalog) • Limited resources to sustain systems post-project.
Medium Term Expenditure Framework (MTEF) for 2024-2027: Programme-Based Budget Estimates for 2024 (Government of Ghana, 2024)	To increase access to quality essential health care and population-based services for all by 2030.	• The Ministry of Health retains sector-wide stewardship, policy formulation, coordination, monitoring, and regulation functions. • Governance is operationalized through programme and sub-programme structures under Management and Administration, including Health Research, Statistics and Information Management. • Oversight challenges are acknowledged, including weak health information management systems,	• Interoperability is not articulated as a formal framework. However, the budget explicitly supports linking the NHIS information system to DHIMS2, expansion and monitoring of Health Electronic Medical Records System (LIGHTWAVE), and coordination of standards, repositories, and health information policies through the Health Research, Statistics and Information Management sub-programme.	• Poor health information management systems • Inadequate and slow deployment of ICT infrastructure • Limited funding for recurrent and capital expenditure • Delays in NHIS reimbursements • Fragmented ICT investments across agencies • Weak coordination, long procurement and audit processes • Insufficient resources to support monitoring, evaluation, and system integration activities.

		delays in agency performance reporting, and limited resources for monitoring and evaluation.		
Health Information Management System Standard Operating Procedures (4th Edition) (Ghana Health Service, 2020)	Provide a formalized system to guide data collection, collation, storage, analysis, reporting and utilization to obtain quality information to facilitate decision making in the Service.	- Defines a multi-level governance structure for health information management across facility, district, regional, and national levels. Assigns clear accountability to facility heads, District Directors of Health Services, Regional Directors of Health Services, the Director-General of GHS, Centre for Health Information Management (CHIM), and the Health Information Technical Working Group (HITWG). - Establishes mandatory data validation teams at all levels and formal approval and sign-off procedures in DHIMS2, including enforcement of data ownership and accountability through electronic sign-off and data lock rules.	- Establishes DHIMS2 as the national data repository and master facility registry. - Provides operational guidelines for automation of datasets from other systems including eTracker, hospital EMRs, GhiLIMS, PBMIS, HRIMS, and other sector systems into DHIMS2. - Specifies validation, synchronization, update, and locking protocols to enable controlled data exchange and system interoperability, without defining new technical standards beyond approved system compatibility.	Does not articulate explicit policy barriers. However, the SOP acknowledges operational constraints, including: - facilities without data entry capacity - reliance on manual reporting - need for clearance before EMR procurement - capacity gaps in data management skills - infrastructure limitations, - risks to data quality arising from non-compliance with prescribed procedures.
Ghana's health sector low in cybersecurity maturity – CSA cautions	Heighten staff awareness of basic cybersecurity and ensure adherence to	The Cyber Security Authority (CSA) assessed cybersecurity maturity in 15 health entities (8 public hospitals, 3 private	The article does not outline specific interoperability frameworks.	Critical vulnerabilities were found (no password encryption, outdated software, susceptibility to DDoS, web server

(Cyber Security Authority, 2024) Link	regulations to mitigate risks.	hospitals, 4 medical labs), highlighting weak governance of cybersecurity practices in health institutions. • CSA urged collaboration among hospitals, healthcare providers, technology experts, and policymakers to establish robust data protection frameworks and improve cybersecurity governance.	• It calls for frameworks for data protection and collaborative strategies to safeguard patient data but does not specify technical or standards-based interoperability plans.	misconfiguration, lack of HTTPS enforcement), indicating low cybersecurity maturity and insufficient implementation of security directives (such as the Critical Information Infrastructure Directive). • Lack of robust cybersecurity governance and insufficient capacity-building were highlighted as barriers to protecting health data.
Fortifying Ghana's Healthcare Against Cyber Threats: An Urgent Call to Action (IIPGH, 2025) Link	Fortify Ghana's healthcare sector against cyber threats and enhance cybersecurity measures to protect patient data and ensure continuity of essential medical services.	• Highlights absence of robust cybersecurity governance in healthcare institutions. • Calls for improved governance through collaboration among government agencies (e.g., Cyber Security Authority), healthcare providers, and cybersecurity experts. • Recommends establishment of clear leadership, accountability, and multi-stakeholder coordination for national and institutional cybersecurity policies.	• No specific technical interoperability framework is defined. • Article emphasizes need for integration of cybersecurity into digital health systems and adoption of secure data exchange practices. • It suggests that legislative frameworks (Cybersecurity Act 2020; Data Protection Act 2012) should inform secure interoperability but does not specify standards or architecture.	• Critical gaps in cybersecurity readiness including phishing, ransomware, and insider threats in health systems. • Lack of staff cybersecurity awareness and training, outdated systems, weak technical safeguards (encryption, multi-factor authentication), absence of incident response plans, and insufficient enforcement of cybersecurity standards across health facilities. • Legislative frameworks exist but implementation and compliance are weak.

Health Sector ICT Policy and Strategy (Ministry of Health, 2005)	The development and implementation of an information and communication technology (ICT) programme to transform the entire health delivery system and to support the achievement of the vision of the health sector.	• Establishes MoH as the policy lead and steward for health sector ICT, with implementation delegated to agencies (GHS, • Teaching Hospitals, NHIS, regulatory councils) and coordination through proposed structures including a Health Information and Communication Technology Advisory Committee (H-ICT) and ICT task forces within agencies. • Identifies weak corporate commitment, fragmented agency programmes, limited coordination with private sector providers, and absence of enforceable governance arrangements as systemic weaknesses.	• Proposes a sector-wide Health Information Management Systems Network evolving from stand-alone systems to an integrated eHealth information system. • Calls for open architecture, modular design, compliance with international standards (e.g. ICD, DRGs), unique patient identifiers within the health sector, standardized coding and classification, and integration across public, mission, and private providers. • Envisions interoperability across clinical, public health, insurance, pharmacy, and regulatory systems, aligned with ICT4AD.	• Absence of national standards for health data, coding, and interoperability • Lack of legal frameworks for privacy, confidentiality, and data protection • Weak telecommunications infrastructure; inadequate ICT human resource capacity • Poor planning and budgeting for ICT; fragmented procurement of hardware and software; lack of enforcement mechanisms • Weak integration of private sector data into national health information flows.
--	--	--	---	--