Online-Journals.org

iJOE International Journal of Online and Biomedical Engineering

iJOE | eISSN: 2626-8493 | Vol. 22 No. 11 (2026) | OPEN ACCESS

https://doi.org/10.3991/ijoe.v22i11.63318

SPECIAL FOCUS PAPER

Regulating AI-Based Digital Healthcare Systems: Economic Sustainability, Data Protection, and Legal Accountability in Bahrain and the European Union

Raed Alnimer (✉)

Royal University for Women, Manama, Kingdom of Bahrain

ralnimer@ruw.edu.bh

ABSTRACT

The rapid integration of artificial intelligence (AI) into digital healthcare systems generates transformative efficiencies in diagnostics, clinical decision support, and population health management, while producing unresolved legal, ethical, and economic challenges. This paper presents a comparative doctrinal analysis of AI healthcare regulatory frameworks in Bahrain and the European Union (EU), focusing on three dimensions: civil liability and algorithmic accountability, health data protection and automated processing governance, and economic sustainability of regulatory compliance. Bahrain's emerging framework rests on the Personal Data Protection Law (PDPL, Law No. 30 of 2018), NHRA supervisory authority, the Digital Health Integration System (DHIS), and Vision 2030; a standalone 38-article AI regulation law was approved by the Shura Council in April 2024 but not yet enacted. The EU operates a mature multi-layered regime comprising the AI Act (Regulation EU 2024/1689), GDPR, MDR, and the revised Product Liability Directive. Applying doctrinal and functional comparative methodology, this paper identifies three critical gaps in Bahrain: (i) the blanket prohibition on automated processing of sensitive personal data, rendering clinical AI presumptively unlawful; (ii) the absence of a civil liability instrument for AI-caused patient harm; and (iii) the lack of sector-specific healthcare AI standards.

KEYWORDS

artificial intelligence (AI) regulation, digital healthcare, Bahrain, European Union (EU), legal accountability, data protection, economic sustainability, algorithmic, comparative law, GCC

1 INTRODUCTION

The incorporation of artificial intelligence (AI) technologies into healthcare constitutes one of the most consequential technological developments of the current century [2]. AI systems are now deployed across clinical applications—from radiological image analysis and pathology diagnosis to real-time patient triage, predictive risk stratification, personalized treatment prescription, and population health

Alnimer, R. (2026). Regulating AI-Based Digital Healthcare Systems: Economic Sustainability, Data Protection, and Legal Accountability in Bahrain and the European Union. *International Journal of Online and Biomedical Engineering (iJOE)*, 22(11), pp. 22–35. https://doi.org/10.3991/ijoe.v22i11.63318

Article submitted 2026-08-22. Revision uploaded 2026-10-06. Final acceptance 2026-10-09.

© 2026 by the authors of this article. Published under CC-BY.

monitoring—carrying substantial potential to address growing healthcare demand, aging populations, and resource constraints. They also raise fundamental legal questions existing regulatory regimes were not designed to answer: What is the civil liability of an AI diagnostic system's manufacturer where a patient suffers harm? How can meaningful informed consent be secured when patients cannot understand the rationale behind algorithmic outputs? How should health data—simultaneously the engine of AI innovation and the most sensitive category of personal data—be governed? And how can regulators promote the economic sustainability of healthcare AI investment without compromising legal enforceability?

These challenges are especially acute in jurisdictions undergoing rapid digital transformation, such as Bahrain, and in the world's most advanced AI regulatory jurisdiction, the EU. Bahrain has made remarkable strides in digital health governance: the I-SEHA National Health Information System (2014), the BeAware Bahrain telemedicine application, the 2024 Digital Health Integration System (DHIS), and a cloud-first infrastructure policy grounded in Vision 2030 together constitute a regionally leading digital health ecosystem [1]. NHRA has modernized its e-regulatory services [3], and the Personal Data Protection Law (PDPL) of 2018 established a foundational data protection framework [4]. The Shura Council's unanimous approval in April 2024 of a draft standalone AI law of 38 articles is an unprecedented GCC development [5]. Nonetheless, critical gaps persist, particularly regarding AI-based clinical liability and automated processing of health data.

The EU has established the world's first comprehensive, legally binding horizontal AI regulatory framework. The AI Act (Regulation EU 2024/1689), in force since 1 August 2024, applies a risk-stratified governance model to all AI systems on the EU market, operating alongside the GDPR, MDR 2017/745, and the revised Product Liability Directive to produce a coherent multi-layered architecture addressing transparency, human oversight, conformity assessment, data governance, and algorithmic explainability [2]. A comparative legal examination of these two systems—one mature and comprehensive, the other emergent but ambitious—can generate insights of value not only for Bahrain but for all GCC states seeking to govern healthcare AI through the lens of economic sustainability, data protection, and legal accountability.

1.1 Research objectives (RO)

This paper pursues the following four specific RO:

RO1: To map and critically analyze the existing regulatory frameworks governing AI-based digital healthcare systems in Bahrain and the EU, identifying the principal legislative instruments, enforcement mechanisms, and institutional actors in each jurisdiction.

RO2: To conduct a systematic comparative analysis of the two frameworks across three dimensions—health data protection, civil liability and algorithmic accountability, and economic sustainability of compliance—identifying convergences, divergences, and regulatory gaps.

RO3: To evaluate the specific legal impediments to the deployment of AI-based clinical systems in Bahrain's private healthcare sector under the current PDPL and to assess whether the draft AI law of 2024 adequately addresses these impediments.

RO4: To formulate targeted, actionable reform recommendations for Bahrain, informed by EU regulatory experience but adapted to the specific constitutional, institutional, and socio-economic context of the Kingdom, and extensible to the wider GCC.

2 LITERATURE REVIEW

Academic engagement with AI regulation and healthcare law has expanded substantially since 2020, driven by the maturation of clinical AI and accelerating legislative agendas. Three thematic clusters characterize the literature and define the research gap this paper addresses: comparative regulatory architecture, data protection and consent, and legal liability.

2.1 Comparative regulatory architecture

The global regulatory landscape of healthcare AI is highly heterogeneous. Three dominant governance paradigms can be identified [6] identify three dominant governance paradigms: sector-specific medical device regulation (the EU MDR; the FDA's Software as a Medical Device (SaMD) pathway); horizontal AI-specific regulation (the EU AI Act); sector-specific medical device regulation (the EU MDR; the FDA's SaMD pathway); horizontal AI-specific regulation (the EU AI Act); and soft-law frameworks (OECD AI Principles; UNESCO AI Ethics Recommendations). It has been argued that no single paradigm suffices alone and that effective governance requires layered architectures addressing the technical, clinical, ethical, and legal dimensions of AI simultaneously [6]. This is further grounded in clinical practice by evidence that algorithmic opacity—the inability of clinicians and patients to understand AI reasoning—is structurally incompatible with informed consent and evidence-based shared decision-making [7].

At the EU level, the first systematic legal analysis of the AI Act's implications for digital medicine [8] affirms the classification of medical AI as high-risk while identifying interpretive uncertainties at the AI Act/MDR interface. This has since been partially addressed by the joint MDCG/EU AI Board FAQ of 2025 [9], which confirms that compliance with one framework cannot substitute for the other, thereby requiring dual conformity pathways. This dual compliance burden is directly relevant to the economic-sustainability analysis presented in Section 4.4.

Research on AI governance in the GCC remains nascent. The most comprehensive comparative analysis of national AI strategies across Gulf states to date [10] concludes that Bahrain leads the region in digital governance maturity and data protection development. However, it notes that sector-specific healthcare AI governance is absent across the GCC—a critical gap at precisely the intersection of AI capability and patient safety risk, which this paper directly addresses.

2.2 Data protection and health data governance

The relationship between data protection law and healthcare AI has attracted significant scholarly attention. Research argues that data protection statutes, including the GDPR, were not architected for the emergent risks of AI-generated health insights—particularly re-identification of de-anonymized datasets and sensitive health inferences drawn algorithmically from ostensibly non-health data [11]. Also, research extends this by identifying fundamental difficulties in operationalizing the GDPR's right to explanation for machine learning models whose outputs do not correspond to human-interpretable reasoning chains [12].

In comparative GCC law, [13] establishes that Bahrain's PDPL is the most comprehensive data protection instrument in the Gulf and was deliberately modelled on GDPR principles, but identifies a critical divergence: the PDPL's general prohibition on automated processing of sensitive personal data, including health data, is more restrictive than the GDPR and lacks the GDPR's calibrated exceptions for clinical necessity. This creates what this paper terms the "automated processing gap"—examined in Section 4.2.

Recent research also highlights integrating technical and legal safeguards for health data governance. Past research demonstrated that blockchain-based cloud EHR architectures can materially enhance data security, regulatory compliance, and interoperability while preserving patient privacy, showing that technical infrastructure choices interact significantly with legal frameworks—an interaction directly relevant to the evaluation of Bahrain's DHIS in Section 4.1 [14].

2.3 Legal liability for AI-caused harm

Artificial intelligence-generated liability in healthcare is perhaps the most doctrinally underdeveloped area of the field. Research analyzes the EU's emerging liability architecture, finding that while the revised Product Liability Directive and proposed AI Liability Directive represent significant advances, fundamental challenges remain regarding causation in multi-party clinical AI workflows where harm arises from interactions between AI systems, clinical protocols, and individual judgments [15]. Also, research examines the practical uncertainties facing hospitals as AI deployers, concluding that current frameworks generate significant liability exposure absent clear standards of care for AI-assisted practice [16].

Several research offer the most comprehensive analysis of the AI Act's implications for digital health liability, identifying the lack of a unified AI liability framework as a structural weakness the proposed AI Liability Directive seeks to remedy through a rebuttable causation presumption [17]. From a GCC perspective, [18] provides the foundational analysis of civil liability in medical negligence across Gulf legal systems, showing that the standard-of-care doctrine, developed for individual physician-patient relationships, is ill-suited to systemic harms from AI system failures.

A notable gap in the literature—directly addressed by this paper—is the absence of systematic comparative analysis of AI healthcare liability frameworks between the GCC and the European Union.

3 RESEARCH METHODOLOGY

This paper employs two complementary methodological approaches: doctrinal legal research and comparative law methodology.

Doctrinal legal research is defined [19] as "the systematic analysis and explication of legal rules, their logical consistency, and their application by means of authoritative legal sources including legislation, regulatory instruments, and judicial decisions." This is appropriate here because the paper's central inquiry concerns the content and normative quality of Bahrain's and the EU's legal frameworks, not empirically measured outcomes or behavioral effects.

Comparative law methodology [20] involves identifying functionally equivalent legal institutions across jurisdictions and analyzing how each resolves an equivalent practical problem—here, the governance of AI-based digital healthcare. The Bahrain-EU comparison is productive because it combines deliberate normative

convergence (the PDPL was explicitly modelled on GDPR principles) with significant divergence in enforcement architecture, liability mechanisms, and legislative maturity—a combination sometimes termed "inspired transplant," enabling analysis of both the limits of legislative borrowing and the conditions necessary for transplanted norms to function effectively [20].

Each objective is addressed through a specific application of these methodologies. RO1 uses doctrinal analysis of the primary legal instruments below, read against secondary regulatory guidance from the European Commission, MDCG, EU AI Board, and Bahraini authorities. RO2 uses structured comparative analysis applying the functional method [20] to each of the three dimensions—data protection, civil liability, and economic sustainability—identifying convergence and divergence at the level of both principle and institutional implementation. RO3 uses close doctrinal reading of the PDPL's automated-processing provisions against representative clinical AI use cases (diagnostic imaging, predictive risk stratification, automated triage) to determine lawfulness under the current statutory text. RO4 uses a normative-comparative method evaluating EU solutions for functional transplant ability to Bahrain's institutional and socio-legal context, consistent with legal-transplant scholarship [20].

Primary sources analyzed: from Bahrain, the PDPL [4], Ministerial Resolution No. 45/2022 [21], the draft AI Law [5], and NHRA instruments [3]; from the EU, the AI Act [22], GDPR [23], MDR [24], and the revised Product Liability Directive [25]. Secondary sources include peer-reviewed legal and interdisciplinary scholarship and regulatory guidance from the European Commission, MDCG, EU AI Board, and Bahraini authorities. The paper does not employ empirical data collection, clinical evaluations, or primary survey research.

4 RESULTS

This section presents the comparative findings across four dimensions: regulatory architecture, health data protection, legal liability and accountability, and economic sustainability. Each subsection sets out the applicable EU and Bahraini framework in turn, establishing the basis for the synthesis in Section 5.

4.1 Regulatory architecture: Bahrain and the European Union

The EU's multi-layered framework. The EU has constructed the most comprehensive multi-layered regulatory framework for healthcare AI worldwide. Three instruments apply concurrently to clinical AI systems, as confirmed by the MDCG/EU AI Board joint FAQ of 2025 [9].

First, the MDR (Regulation EU 2017/745) [24] governs the safety and performance of medical device software for diagnostic, monitoring, or therapeutic purposes. AI systems classified as SaMD must undergo third-party conformity assessment by a notified body, covering clinical evaluation, risk management, and post-market surveillance.

Second, the GDPR (Regulation EU 2016/679) [23] governs the collection, processing, storage, and transfer of patient health data. Article 9 categorizes health data as sensitive, requiring additional safeguards; processing is lawful only on specific bases, including explicit consent or medical necessity. Article 22 confers the right not to be subject to decisions based solely on automated processing producing legal or similarly significant effects, subject to exemptions including explicit consent.

Third, the AI Act (Regulation EU 2024/1689) [22], in force since 1 August 2024, introduces a risk-stratified governance model. Medical AI—diagnostic software, patient triage, and eligibility-assessment tools—is high-risk, requiring risk management systems, quality training data, technical documentation, transparency, human oversight, robustness, and cybersecurity safeguards; vulnerable-individual exploitation and biometric manipulation are prohibited across all sectors. Mandatory conformity assessment applies from 2 December 2027 (standalone systems) and 2 August 2028 (embedded AI) [22].

Fourth, the revised Product Liability Directive (Directive EU 2024/2853) [25] extends product liability to AI systems, covering death, personal injury, and medically recognized psychological harm, and shifts the burden of proof to manufacturers to demonstrate absence of defect where causation is plausible. The proposed AI Liability Directive will supplement this with a rebuttable presumption of causation for AI Act non-compliance. Research argues that healthcare operators should engage proactively with these requirements ahead of their full legal effect, treating compliance as ongoing trustworthiness assessment rather than a point-in-time exercise [26].

Bahrain's emerging regulatory architecture. The PDPL (Law No. 30 of 2018) [4], effective from 1 August 2019, is the foundational data protection instrument. Modelled on GDPR principles, it incorporates transparency, purpose limitation, data minimization, accuracy, storage limitation, and security requirements, and categorizes health data as sensitive personal data warranting heightened protection. Article 5 requires explicit consent for health data processing, while Ministerial Resolution No. 45 of 2022 [21] establishes the authorization procedure for health data processing by regulated entities. Enforcement rests with the Personal Data Protection Authority (PDPA).

The National Health Regulatory Authority (NHRA), established under Vision 2030, serves as the independent regulator of Bahrain's private healthcare sector, with competences spanning facility and professional licensing, medical device registration, quality standards, and increasingly digital health innovation governance [3]. NHRA directives require regulated facilities to designate a Data Protection Guardian (DPG)—a requirement with practical significance for AI deployment governance.

The most significant recent development is the Shura Council's unanimous April 2024 approval of a draft standalone AI law of 38 articles [5], imposing transparency and human oversight obligations, prohibiting certain harmful AI uses, and introducing criminal sanctions of up to three years' imprisonment or BD 2,000 fines. A comprehensive National AI Framework, due by 2026, will operationalize these provisions, coordinated by the Information and eGovernment Authority (ICTGC).

The supporting digital health infrastructure includes I-SEHA (the national EHR system), the 2024 DHIS, a legally recognized telemedicine framework, and cloud infrastructure centered on the AWS Bahrain region—together one of the Gulf's most advanced digital health foundations [27].

4.2 Data protection: comparative analysis

Foundational principles: convergence. A notable feature of the Bahrain-EU comparison is the deliberate convergence at the level of foundational data protection principles. The PDPL incorporates the core GDPR principles of transparency, purpose limitation, data minimization, accuracy, storage limitation, and security [4]. Both instruments treat health data as a special category warranting heightened protection, and both confer rights of access, rectification, erasure, and objection. This reflects the Bahraini legislator's intention to align with international best practice, facilitate data exchange with GDPR-governed jurisdictions, and attract foreign

investment in digital health. Similar GDPR-inspired convergence is observable across GCC frameworks [13], suggesting an emerging regional consensus at the level of principles, though not yet institutional implementation.

The automated processing divergence. The most consequential divergence concerns automated processing of health data—the functional core of healthcare AI. Under GDPR Article 22 [23], automated individual decision-making is regulated rather than prohibited: the right not to be subject to wholly automated decisions producing significant effects is qualified by exemptions for contract necessity, explicit consent, and member-state legal authorization. Article 9(2) provides further legal bases for processing sensitive health data, including medical diagnosis, treatment, and health-system management. The AI Act [22] adds a mandatory human oversight requirement for high-risk AI, making fully autonomous clinical decision-making structurally impermissible. The net effect is a graduated approach: automated processing of health data is lawful under appropriate legal bases, provided human oversight is maintained for high-risk decisions.

Bahrain's PDPL [4], by contrast, contains a general prohibition on automated processing of sensitive personal data, expressly including health data (Article 5), with no statutory exception for clinical necessity, explicit consent, or AI-specific use cases. Neither the 2022 Ministerial Resolution [21] nor the 2024 draft AI law [5] has introduced such an exception. The practical consequence is stark: diagnostic imaging AI, predictive risk algorithms, automated triage, and drug interaction checkers—the core applications of clinical AI—appear presumptively unlawful under the existing PDPL when deployed in Bahrain's private healthcare sector. This "automated processing gap" constitutes the most critical single regulatory impediment to AI-based digital healthcare in Bahrain.

Cross-border data flows. Both frameworks restrict cross-border transfers of health data, given its heightened sensitivity. GDPR Chapter V [23] permits international transfers only where adequate protection is guaranteed—via adequacy decision, standard contractual clauses, binding corporate rules, or other approved mechanisms. Bahrain has not yet obtained an EU adequacy decision, so transfers between EU-based AI developers and Bahraini health institutions require individual mechanisms such as GDPR-compliant SCCs—a practical friction point for internationally contracted AI diagnostics services. The PDPL [4] correspondingly restricts outbound transfers to countries ensuring adequate protection or where the PDPA has issued specific authorization. Absent a formal adequacy arrangement or bilateral data governance agreement, this bilateral constraint significantly complicates cross-border health AI development relationships between Bahrain and EU-based technology providers.

4.3 Legal liability and accountability

EU liability architecture. The EU's liability framework for AI-caused healthcare harm has evolved significantly, since conventional product liability and malpractice doctrine are structurally inadequate for AI's specific features. The revised Product Liability Directive (Directive EU 2024/2853) [25] constitutes the foundation of the EU liability architecture. It extends the statutory definition of "product" to software and digital outputs, making manufacturers and developers of defective AI systems strictly liable for death, personal injury, and medically recognized psychological harm—categories responsive to the most common forms of AI-mediated clinical error. Significantly, it reverses the ordinary burden of proof in favor of patients where AI

system opacity makes it impractical for claimants to establish defect without access to system internals.

The proposed AI Liability Directive introduces a further innovation: a rebuttable presumption of causal nexus between AI Act non-compliance and the harm suffered. Where an AI system fails the transparency, accuracy, or human oversight requirements of the AI Act [22], and harm results in circumstances consistent with that non-compliance, causation is presumed unless rebutted—addressing the epistemic problem identified by Wachter et al. [12]: patients harmed by AI systems typically lack access to algorithmic reasoning chains, making causal proof under conventional doctrine practically impossible.

Healthcare institutions deploying AI bear a duty of care to validate systems against regulatory requirements, maintain post-deployment surveillance, ensure clinician competency, and preserve meaningful human oversight. Individual clinicians face potential malpractice liability for failing to exercise professional judgment on AI recommendations—whether through uncritical reliance or unjustified disregard. Notably, despite this sophisticated architecture, no AI system has yet been the subject of successful patient harm litigation in European courts [16–17], reflecting both the technology's novelty and the evidential challenges the AI Liability Directive seeks to address.

Bahrain's accountability gap. Bahrain currently lacks any liability instrument functionally equivalent to the EU's revised PLD or AI Liability Directive. Three existing legal doctrines potentially govern accountability for AI-generated clinical error, each with significant limitations in the AI context.

First, tortious liability under Bahrain's Civil Code (Decree-Law No. 19 of 2001) [28] affords patients a right to compensation for damage from negligent acts or omissions. However, establishing negligence for AI-generated error requires proof that the relevant actor—developer, deployer, or clinician—failed to exercise reasonable care, a burden complicated by machine learning opacity and the absence of defined standards of care for AI-assisted practice.

Second, medical malpractice doctrine holds practitioners to a professional standard of care. As Al Majed [18] demonstrates, this standard in Gulf legal systems was developed for individual physician-patient relationships and has not been extended to multi-party AI clinical workflows, leaving unresolved whether a clinician is liable for adopting AI recommendations without adequate validation or for not adopting ones that would have improved outcomes.

Third, the PDPL [4] provides administrative and criminal enforcement for data protection violations, including financial penalties and criminal sanctions. These protect against unlawful data processing but afford no compensatory remedy to patients harmed by AI clinical errors. The criminal sanctions in the 2024 draft AI law [5]—up to three years' imprisonment and BD 2,000 fines—similarly address regulatory non-compliance rather than patient compensation. The gap is further complicated by the PDPL's automated processing prohibition: violating deployments would constitute unlawful conduct, potentially facilitating liability claims in principle but providing no compensatory framework in practice.

Informed consent in AI-mediated healthcare. Informed consent presents a structurally parallel challenge in both jurisdictions, though the governing legal architecture differs substantially. Three AI-specific consent questions arise in clinical practice: whether patients must be informed that AI has participated in their care; what degree of algorithmic explanation is required for meaningful consent; and whether patients may refuse AI participation in their clinical pathway.

The EU framework addresses these questions through a layered approach. GDPR Article 22 [23] confers a right to human review of automated decisions producing significant effects, implicitly requiring disclosure of AI involvement. The AI Act [22] mandates that high-risk AI systems be accompanied by meaningful instructions for use, enabling clinicians and, indirectly, patients to understand AI function and limitations. Emerging academic discourse on attribute-level consent—allowing patients to specify consent for different AI applications of their health data—has not yet been legislatively operationalized in the European Union.

In Bahrain, the PDPL's explicit consent requirement for health data processing [4] provides a legal basis for developing AI-specific consent practices, but existing guidance does not address the distinctive features of AI-mediated care. There is presently no regulatory guidance from NHRA [3] or the PDPA on the form, content, or process of consent for AI-assisted diagnosis or treatment planning, and the draft AI law [5], while imposing transparency obligations on developers, does not address patient-level consent for AI clinical participation—a gap that is both a patient rights concern and a clinical risk management vulnerability for providers.

4.4 Economic sustainability of AI-based digital healthcare systems

Regulatory compliance as an economic variable. The economic viability of healthcare AI is materially conditioned by regulatory compliance costs. Disproportionate, uncertain, or duplicative obligations inflate market-entry costs and disadvantage smaller providers and startups relative to large incumbents with dedicated regulatory affairs functions.

In the EU, the AI Act's [22] high-risk classification for most clinical AI entails substantial compliance expenditure: risk management systems, technical documentation, data governance, post-market surveillance, and mandatory notified-body assessment. The MDCG/EU AI Board FAQ of 2025 [9] confirms dual compliance is required with both the AI Act and MDR [24], generating cumulative requirements SME developers have criticized as significant market-entry barriers. While the risk-tiered structure relieves lower-risk applications, most clinically impactful systems bear the full compliance burden.

In Bahrain, the economic sustainability problem has a different character: the challenge is not over-regulation but regulatory uncertainty combined with a structural prohibition. The PDPL's ban on automated processing of health data [4] effectively forecloses commercialization of the most economically significant clinical AI applications, while the absence of sector-specific AI standards creates compliance uncertainty, deterring both domestic facilities and international health technology companies from the Bahraini market. Regulatory gaps thus impose economic costs not only through compliance expenditure but through foregone innovation, efficiency gains, and competitive positioning in the regional health technology market.

Innovation-regulation balance and public trust. Effective AI healthcare regulation requires calibrating between regulatory laxity—risking patient harm and erosion of public trust—and regulatory excess, which chills innovation and forecloses efficiency gains clinical AI could otherwise deliver. The EU's risk-tiered AI Act approach [22] reflects a sophisticated attempt at this calibration: minimal-risk applications bear no AI-Act obligations, limited-risk applications face transparency requirements, and high-risk clinical applications face the full compliance architecture—an advance, however imperfect at the boundaries, over blanket prohibition or permissiveness.

Bahrain currently occupies neither end of the spectrum sensibly: the existing framework neither permits clinical AI under appropriate safeguards nor provides a structured path to lawful deployment. The anticipated National AI Framework (2026) offers an opportunity for calibrated, evidence-based architecture, with the AI Act's Article 57 sandbox provision [22] offering a valuable model for Bahrain's ICTGC-led innovation hubs.

Economic sustainability is also conditioned by public and professional trust: opaque or substitutive (rather than augmentative) AI faces adoption resistance, undermining the investment case. Both jurisdictions recognize transparency as a trust-building mechanism, albeit through different instruments [5] [22] [29]. Similarly, they show that AI-, IoT-, and big-data-driven healthcare ecosystems depend for long-term sustainability on robust data governance and cybersecurity safeguards—precisely what legal frameworks seek to institutionalize. Disclosure obligations alone are necessary but not sufficient for trust; they must be accompanied by health literacy and patient advocacy mechanisms enabling patients to exercise disclosure rights meaningfully.

5 DISCUSSION

5.1 Comparative synthesis and reform recommendations

The foregoing analysis reveals a pattern of normative convergence at the level of regulatory principles and institutional divergence at the level of regulatory capacity and legal specificity. Both jurisdictions affirm transparency, human oversight, data protection, proportionality, and patient safety as foundational values, and both have embarked on dedicated AI governance initiatives, but the depth, specificity, and enforceability of the frameworks differ markedly. Table 1 presents the comparative findings across eight regulatory dimensions.

Table 1. Comparative regulatory framework: Bahrain vs. EU (author's analysis)

Dimension	EU	Bahrain	Gap
Primary AI instrument	AI Act; revised PLD	Draft AI Law (2024); Nat'l AI Framework (2026). [4]	Medium
Health data protection	Art. 9(2): special category; consent/necessity basis	Art. 5: explicit consent; sensitive category; broader, less nuanced. [5]	Critical
Automated processing	Permitted with safeguards; human oversight for high-risk	Prohibited for sensitive data; no clinical exception—most clinical AI is presumptively unlawful. [13]	Critical
Risk classification	Four-tier: medical AI = high-risk	Not yet adopted; NHRA device registration only. [22]	High
Civil liability instrument	Revised PLD: strict liability; AI Liability Directive presumption	Civil Code general tort only; no compensation pathway. [23]	Critical
Conformity assessment	Mandatory notified-body assessment (2027/2028)	Nascent; no AI-specific system	High
Enforcement	AI Office; DPAs; fines of €35m/7% turnover	PDPA; NHRA; ICTGC; up to 3yr/BD 2,000—less graduated. [25] [28]	Medium
Informed consent	Art. 22 review right; mandatory instructions for use	Explicit consent required; no AI-specific guidance.	High

5.2 Reform recommendations for Bahrain

Drawing from the comparative analysis and directly responding to the RO (RO2–RO4), this paper advances five targeted reform recommendations addressed to Bahrain and extensible to GCC jurisdictions.

Recommendation 1: Statutory Exception for Automated Health Data Processing in Clinical AI. The PDPL's blanket prohibition on automated processing of sensitive personal data should be qualified by a statutory exception for AI-based clinical applications, requiring explicit AI-specific consent, NHRA pre-authorization, mandatory audit trails, and human oversight of all AI-generated recommendations before implementation—replicating GDPR Article 9(2) [23] while incorporating the AI Act's oversight requirements [22]. Without this amendment, the PDPL will continue to render the most clinically and commercially significant healthcare AI applications presumptively unlawful.

Recommendation 2: Enactment of a Dedicated AI Civil Liability Instrument. Bahrain should enact a legal instrument providing a clear, accessible compensation pathway for patients harmed by AI clinical systems, incorporated either into the forthcoming standalone AI law or the Civil Code framework [28]. It should include a modified strict liability standard for certified AI medical devices modelled on the revised PLD [25], a rebuttable causation presumption for regulatory non-compliance modelled on the proposed EU AI Liability Directive, mandatory operator insurance, and a litigation disclosure obligation for AI system documentation. The criminal penalties in the 2024 draft AI law [5] do not serve these compensatory functions and should not substitute for a civil liability framework.

Recommendation 3: Establishment of a Formal AI Healthcare Regulatory Sandbox. NHRA and the PDPA should jointly establish a formal AI healthcare regulatory sandbox, modeled on the AI Act's Article 57 innovation sandbox provision [22], allowing controlled testing of clinical AI under regulatory supervision before full compliance obligations attach. It should offer time-limited exemptions from the automated processing prohibition during supervised trials, require participants to share trial data with regulators, and generate an evidentiary base for proportionate permanent frameworks—simultaneously stimulating innovation, building regulatory capacity, and positioning Bahrain as a regional digital health innovation hub.

Recommendation 4: Development of Healthcare-Specific AI Standards. NHRA and ICTGC should develop, in consultation with clinical professional associations, health technology developers, and patient advocacy bodies, sector-specific standards for clinical AI covering: data governance and quality requirements; algorithmic performance metrics and validation protocols; explainability requirements calibrated to clinical context; post-deployment monitoring and adverse event reporting; and clinician training requirements. These standards would give providers the legal certainty necessary for investment decisions, reduce compliance costs through clear benchmarks, and lay the foundation for regulatory harmonization at the GCC level.

Recommendation 5: Leadership of GCC-Level Regulatory Harmonization. Bahrain's established regional leadership in data protection law positions it uniquely to lead the development of a GCC AI Healthcare Regulatory Accord—a multilateral instrument establishing common minimum standards for clinical AI governance across the six GCC states. Fragmented national approaches create barriers to regional healthcare AI markets, raise compliance costs for international developers, and reduce the region's collective attractiveness for health AI investment. A GCC accord modelled on the EU's approach to regulatory coordination, adapted to GCC

governance structures, would generate substantial collective benefits while preserving national regulatory sovereignty at the margin.

6 CONCLUSION

This paper has presented a systematic comparative doctrinal analysis of the legal frameworks governing AI-based digital healthcare in Bahrain and the EU, examining economic sustainability, health data protection, and legal accountability. The analysis reveals that while the EU's multi-layered framework provides coherent, if complex, governance for clinical AI, Bahrain's framework—despite strong digital governance foundations—contains structural gaps in three critical areas: automated processing under the PDPL, civil liability for AI-caused patient harm, and healthcare-specific AI standards. These divergences are matters of institutional capacity and legal specificity rather than values, since foundational principles of transparency, proportionality, and patient safety are shared across both systems. The 2024 draft AI law, though a notable achievement, does not resolve these gaps, leaving the National AI Framework anticipated for 2026 as the principal opportunity to do so. Accordingly, the paper advances five targeted reforms—statutory qualification of the automated processing prohibition, a dedicated civil liability instrument, a healthcare AI regulatory sandbox, sector-specific clinical AI standards, and leadership of GCC-level regulatory harmonization—grounded in Bahrain's specific regulatory gaps and informed by EU experience while remaining attentive to Bahrain's institutional and socio-legal context. As AI becomes increasingly indispensable to modern healthcare, closing this regulatory gap is essential not only for patient safety but also for economic competitiveness and public trust.

7 REFERENCES

[1] Ministry of Health, Kingdom of Bahrain, "MoH initiatives related to Bahrain economic vision 2030: Digital transformation in healthcare," Ministry of Health, Manama, Bahrain, n.d. https://www.moh.gov.bh/Ministry/MOH2030vision?lang=en

[2] European Commission, "Artificial intelligence in healthcare," 2024. [Online]. Available: https://health.ec.europa.eu/ehealth-digital-health-and-care/artificial-intelligence-healthcare_en

[3] National Health Regulatory Authority (NHRA), "NHRA strategy 2021–2025," 2021. [Online]. Available: https://www.nhra.bh/About/Strategy/MediaHandler/GenericHandler/documents/About/Strategy/2021-2025%20NHRA%20Strategy_Englishn.pdf

[4] Kingdom of Bahrain, "Law No. (30) of 2018 with respect to personal data protection," Official Gazette, No. 3365, 2018. https://www.mola.gov.bh/MediaManager/Media/Documents/Laws/Batch3/L3018.pdf

[5] Kingdom of Bahrain, Shura Council, "Draft Artificial Intelligence Regulation Law (38 Articles)," 2024.

[6] S. Gerke, T. Minssen, and I. G. Cohen, "Ethical and legal challenges of artificial intelligence-driven healthcare," in *Artificial Intelligence in Healthcare*, 2020, pp. 295–336. https://doi.org/10.1016/B978-0-12-818438-7.00012-5

[7] D. S. Char, N. H. Shah, and D. Magnus, "Implementing machine learning in health care—Addressing ethical challenges," *New England Journal of Medicine*, vol. 378, no. 11, pp. 981–983, 2018. https://doi.org/10.1056/NEJMp1714229

[8] S. Gilbert, "The EU passes the AI Act and its implications for digital medicine are unclear," *npj Digital Medicine*, vol. 7, Art. no. 130, 2024. https://doi.org/10.1038/s41746-024-01116-6

[9] Medical Device Coordination Group/EU AI Board, "Joint FAQ on the applicability of the AI Act and MDR/IVDR (MDCG 2025-6)," European Commission, 2025. https://health.ec.europa.eu/latest-updates/mdcg-2025-6-faq-interplay-between-medical-devices-regulation-vitro-diagnostic-medical-devices-2025-06-19_en

[10] M. R. Albous, O. R. Al-Jayyousi, and M. Stephens, "AI governance in the GCC states: A comparative analysis of national AI strategies," *arXiv preprint arXiv:2505.02174*, 2025. https://doi.org/10.48550/arXiv.2505.02174

[11] B. Mittelstadt and L. Floridi, "The ethics of big data: Current and foreseeable issues in biomedical contexts," in *The Ethics of Biomedical Big Data*, B. Mittelstadt and L. Floridi, Eds., 2016, pp. 445–480. https://doi.org/10.1007/978-3-319-33525-4_19

[12] S. Wachter, B. Mittelstadt, and L. Floridi, "Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation," *International Data Privacy Law*, vol. 7, no. 2, pp. 76–99, 2017. https://doi.org/10.1093/idpl/ipx005

[13] S. Haidar, "Restrictive approach to data protection in the GCC: Is the EU GDPR a potential inspiration?" *Global Journal of Comparative Law*, vol. 13, no. 2, pp. 227–244, 2024. https://doi.org/10.1163/2211906X-13020005

[14] A. Samala and S. Rawas, "Transforming healthcare data management: A blockchain-based cloud EHR system for enhanced security and interoperability," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 20, no. 2, pp. 46–60, 2024. https://doi.org/10.3991/ijoe.v20i02.45693

[15] M. Duffourc and S. Gerke, "AI-based software in healthcare and the Medical Devices Regulation and AI Act," *EMBO Molecular Medicine*, vol. 15, no. 9, Art. no. e17697, 2023. https://doi.org/10.15252/emmm.202317697

[16] M. Gaddas, M. Dhiab, I. Ben Saida, and H. Ben Saad, "Artificial intelligence in hospitals: Legal uncertainties and emerging risks for patient safety," *EXCLI Journal*, vol. 24, pp. 824–827, 2025. https://doi.org/10.17179/excli2025-8679

[17] I. G. Cohen, T. Evgeniou, S. Gerke, and T. Minssen, "The European Artificial Intelligence Act and the future of digital health," *npj Digital Medicine*, vol. 4, Art. no. 167, 2021. https://doi.org/10.1038/s41746-021-00536-y

[18] Y. S. Ali, "The civil liability from medical negligence of doctors treating complications of coronavirus in the English law: A comparative study with the Iraqi civil law," *International Journal of Law and Society*, vol. 6, no. 1, pp. 1–9, 2023. https://doi.org/10.11648/j.ijls.20230601.11

[19] T. Hutchinson and N. Duncan, "Defining and describing what we do: Doctrinal legal research," *Deakin Law Review*, vol. 17, no. 1, pp. 83–119, 2012. https://doi.org/10.21153/dlr2012vol17no1art70

[20] K. Zweigert and H. Kötz, *An Introduction to Comparative Law*, 3rd ed. Oxford, U.K.: Oxford University Press, 1998.

[21] Kingdom of Bahrain, "Ministerial Resolution No. 45 of 2022 on health data processing authorisation procedures," 2022.

[22] European Union, "Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)," *Official Journal of the European Union*, vol. L, 2024/1689, 2024.

[23] European Union. "Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation)," *Official Journal of the European Union*, vol. L, 119, pp. 1–88, 2016.

[24] European Union, "Regulation (EU) 2017/745 of 5 April 2017 on medical devices (MDR)," *Official Journal of the European Union*, vol. L, 117, 2017.

[25] European Union, "Directive (EU) 2024/2853 of 23 October 2024 on liability for defective products (Revised Product Liability Directive)," *Official Journal of the European Union*, 2024.

[26] J. B. Brodersen *et al.*, "Getting ready for the EU AI Act in healthcare: A call for sustainable AI development and deployment," *arXiv preprint arXiv:2505.07875*, 2025. https://doi.org/10.48550/arXiv.2505.07875

[27] Oxford Business Group, "Bahrain: Smart start—Digital innovation in health care," Bahrain, 2024 Report, 2024. https://oxfordbusinessgroup.com/reports/bahrain/2024-report/education-health-chapter/

[28] Kingdom of Bahrain, "Civil Code, Decree-Law No. 19 of 2001," Official Gazette, Manama, Bahrain, 2001.

[29] A. Abatal, M. Mzili, T. Mzili, K. Cherrat, A. Yassine, and L. Abualigah, "Intelligent interconnected healthcare system: Integrating IoT and big data for personalized patient care," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 20, no. 11, pp. 46–65, 2024. https://doi.org/10.3991/ijoe.v20i11.49893

8 AUTHOR

Dr. Raed Alnimer is an Associate Professor of Law and Vice President Academic at the College of Business and Law, Royal University for Women (RUW), Bahrain. His research spans blockchain law, cybersecurity and contractual liability, comparative private law across Bahrain, the GCC, the UK, and the EU, AI regulation, and digital governance. He contributes actively to international legal scholarship and serves in institutional governance roles at RUW (E-mail: ralnimer@ruw.edu.bh).