Minnesota Journal of Business Law and Entrepreneurship

Volume 2026, No. 2

ISSN: 1540-3270

From Innovation to Market: Legal and Regulatory Challenges in Digital Health Entrepreneurship

Shivam Agarwal[1*], Sushil Pal[2], Sharad Kumar[3], Archana Rani[4]

[1]College of Allied and Healthcare Sciences, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India.

[2]Charak institute of allied and healthcare studies Lucknow, Uttar Pradesh, India.

[3]School of Health and Paramedical Sciences, Vivek University, Bijnor, Uttar Pradesh, India.

[4]School of Health and Paramedical Sciences, Vivek University, Bijnor, Uttar Pradesh, India.

***Corresponding author:** Shivam Agarwal

Abstract:

Digital health entrepreneurship has expanded the routes through which software, connected devices, telehealth platforms, digital therapeutics and artificial intelligence-enabled tools enter healthcare. Unlike general consumer technology, products used for diagnosis, treatment, monitoring or clinical decision support may encounter overlapping requirements for medical-device regulation, clinical evidence, data protection, cybersecurity, professional responsibility and reimbursement. This narrative review examines the principal legal and regulatory challenges that arise as digital health ventures move from an initial concept to market adoption, with particular reference to India, the United States and the European Union. A targeted search of open-access peer-reviewed literature and publicly available regulatory documents was undertaken, prioritising material published or updated from 2017 to August 2026. The evidence indicates that regulatory difficulty is rarely confined to a single approval decision. Intended purpose and product claims may determine whether software is regulated as a medical device; evidence and quality systems influence market authorisation; privacy and cybersecurity obligations shape data architecture; and reimbursement, procurement and interoperability affect adoption after regulatory entry. Artificial intelligence-enabled products add questions concerning dataset relevance, software modification and post-market performance. India has strengthened its framework through the Medical Devices Rules, specific 2026 guidance on medical device software, the Digital Personal Data Protection framework and the Ayushman Bharat Digital Mission. The United States and European Union provide different but similarly layered regulatory pathways. For entrepreneurs, early integration of regulatory, clinical, technical and commercial planning may reduce avoidable redesign and improve readiness for market entry. Regulation is therefore better treated as a lifecycle consideration than as a final compliance step.

Keywords: Artificial intelligence; Data privacy; Medical device software; Reimbursement; Regulatory science; Software as a medical device

Introduction

Digital technologies now support activities ranging from teleconsultation and remote monitoring to clinical decision support, electronic health records and software-based therapeutic or diagnostic functions. The World Health Organization has extended its Global Strategy on Digital Health through 2027, reflecting the continuing importance of digital transformation to health systems.[1] At the same time, startups and other entrepreneurial ventures have become important developers and commercialisers of these technologies. A systematic review of digital health entrepreneurship identified product and business development, regulation, implementation, adoption and evaluation as recurring themes in the field.[2]

Digital health entrepreneurship differs from general software entrepreneurship because failure can affect not only commercial performance but also patient safety, confidentiality and clinical decision-making. Regulatory obligations may therefore begin well before a product is marketed. The intended purpose of a software function can influence whether it is considered a medical device, while the choice of data, claims, users and clinical setting

can alter evidence, privacy, quality and post-market requirements. Lifecycle analyses have consequently argued for ethical and regulatory questions to be addressed from product conception through commercialisation.[3] Telehealth startup literature similarly identifies legal, technological and financial constraints as material barriers to growth.[4]

This review examines the principal legal and regulatory challenges encountered as digital health ventures move from innovation to routine market use. It focuses on product classification, evidence, data governance, cybersecurity, artificial intelligence (AI), liability, reimbursement, interoperability and scale-up, using India, the United States (US) and the European Union (EU) as illustrative regulatory settings. Figure 1 presents the lifecycle framework used for the synthesis.

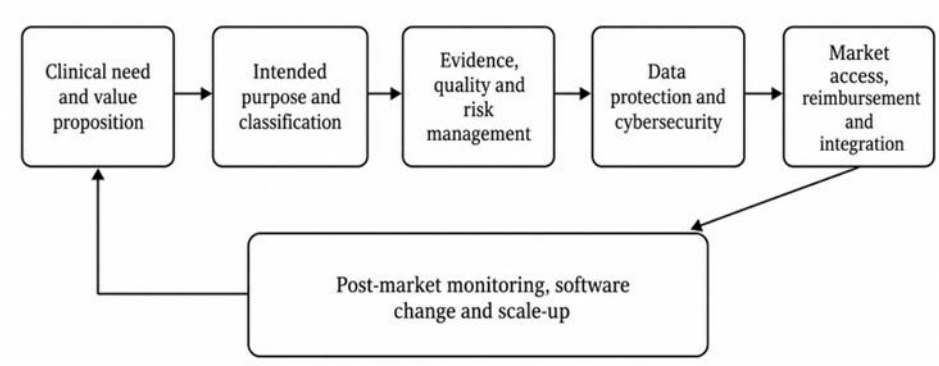

Figure 1. Lifecycle framework for regulatory planning in digital health entrepreneurship. Regulatory questions can arise from definition of intended purpose through post-market monitoring and may require iteration when product claims, data, software or target markets change.

Methods

A structured narrative review was undertaken. Targeted searches were performed in PubMed and PubMed Central and were supplemented by searches of open-access publisher platforms and the official websites of the World Health Organization, US Food and Drug Administration (FDA), US Department of Health and Human Services, US Federal Trade Commission, European Commission, EUR-Lex, Central Drugs Standard Control Organisation (CDSCO), India Code, Ministry of Electronics and Information Technology, and Ayushman Bharat Digital Mission. Searches were last updated on August 27, 2026.

Search terms were used individually and in combination and included “digital health entrepreneurship”, “health-tech startup”, “software as a medical device”, “medical device software”, “AI medical device”, “health data privacy”, “cybersecurity”, “liability”, “reimbursement”, “market access” and “interoperability”. English-language peer-reviewed publications with freely accessible full text and publicly accessible legislation, regulations, policy documents and regulatory guidance were eligible. Material published or updated from January 2017 to August 2026 was prioritised; earlier legal instruments that remained relevant, such as the EU General Data Protection Regulation, were retained. Paywalled publications, commercial market reports, promotional material and sources whose complete text could not be verified were excluded. Because the objective was interpretive synthesis rather than estimation of a pooled effect, no meta-analysis or formal risk-of-bias assessment was performed.

Regulatory classification and market entry

The first consequential regulatory question is whether a digital product, or an individual software function within it, is legally a medical device. In the US, the FDA advises developers to begin with intended use and the statutory device definition. Its Digital Health Policy Navigator distinguishes functions that are likely not devices, functions for which enforcement discretion may apply and functions likely to be the focus of device oversight.[5] This means that two applications using similar technology can have different regulatory positions when their claims and clinical purposes differ.

India applies the Medical Devices Rules, 2017 within the broader drugs and cosmetics framework.[6] CDSCO's July 2026 guidance states that software intended for a medical purpose and meeting the definition of a medical device is regulated as medical device software; it also clarifies that general wellness or healthy-lifestyle software without a medical purpose falls outside that guidance.[7] In the EU, Regulation (EU) 2017/745 applies to qualifying medical device software and uses risk-based classification, including specific rules for software that provides information used for diagnostic or therapeutic decisions.[8]

For entrepreneurs, classification is therefore a product-strategy decision as well as a legal one. A late change in intended use or promotional claims can change the applicable pathway and evidence burden. Early mapping of target markets, intended users and claims may reduce avoidable redevelopment. Table I summarises selected regulatory touchpoints across the three jurisdictions.

Table I. Selected regulatory touchpoints for digital health ventures in India, the United States and the European Union

Domain	India	United States	European Union
Medical-device status	Medical Devices Rules, 2017; 2026 CDSCO guidance clarifies medical device software scope	FDA device definition and digital-health policies; oversight depends on software function and intended use	Medical Device Regulation 2017/745 applies to qualifying medical device software
Risk/classification	Risk-based medical-device classes under MDR, 2017	Product-specific device classification and relevant premarket pathway	Risk-based classification; Rule 11 is important for decision-support software
Personal-data framework	DPDP Act, 2023 and Rules, 2025 with phased commencement; ABDM policy relevant within its ecosystem	HIPAA applies according to covered-entity/business-associate status; FTC rules may apply outside HIPAA	GDPR applies to personal data; health data receive special-category protection
AI-enabled products	Medical-device requirements apply when AI software meets the device definition; product-specific guidance should be checked	PCCP pathway can address certain planned modifications to AI-enabled device software functions	AI Act overlays sectoral law for qualifying high-risk systems; product-integrated high-risk rules have a transition period
Cybersecurity	Risk management and applicable data/security obligations depend on product and ecosystem	FDA premarket cybersecurity guidance addresses devices with cybersecurity risk	Cybersecurity obligations arise through medical-device, data-protection and other applicable EU frameworks
Interoperability/data ecosystem	ABDM promotes federated, consent-based and interoperable health information exchange	Interoperability expectations depend on product, purchaser and applicable federal programmes	EHDS establishes a phased framework for electronic health data exchange and EHR-system requirements

]. ABDM, Ayushman Bharat Digital Mission; AI, artificial intelligence; CDSCO, Central Drugs Standard Control Organisation; DPDP, Digital Personal Data Protection; EHR, electronic health record; EU, European Union; FDA,

US Food and Drug Administration; GDPR, General Data Protection Regulation; HIPAA, Health Insurance Portability and Accountability Act; MDR, Medical Devices Rules/Medical Device Regulation according to jurisdiction; PCCP, predetermined change control plan.

Clinical evidence, quality and software change

Technical performance alone does not establish clinical utility. Evidence should be proportionate to the product's intended purpose, risk and role in decision-making. Open-access analyses of software as a medical device emphasise the importance of clinical validation, patient-centred outcomes and continuing oversight, particularly when software changes after deployment.[9] For a startup, this has a practical consequence: data collected for prototype development may not be sufficient for regulatory evaluation or institutional procurement if the study population, comparator, workflow or outcome does not match the final claim.

Software also changes more frequently than many conventional medical devices. Version control, validation, complaint handling, risk management and post-market surveillance therefore need to be designed into the development process. For AI-enabled device software functions, the FDA's final guidance on predetermined change control plans describes how specified future modifications, the methods used to develop and validate them, and their expected effects can be described in a marketing submission.[10] This does not remove the need for oversight; rather, it creates a structured route for certain anticipated modifications. Startups should consequently distinguish ordinary product iteration from changes that may alter clinical performance, intended use or regulatory status.

Data governance, privacy and cybersecurity

Digital health ventures often depend on identifiable or potentially identifiable health information for service delivery, analytics, model development or product improvement. Legal duties vary substantially by jurisdiction and by the relationship between the company, the individual and the healthcare organisation.

India's Digital Personal Data Protection Act, 2023 establishes a general framework for processing digital personal data.[11] The Digital Personal Data Protection Rules, 2025 were notified in November 2025 with phased commencement, so the operative obligations should be checked against the relevant implementation date and processing context.[12] Within the Ayushman Bharat Digital Mission ecosystem, the Health Data Management Policy adopts a federated architecture and describes security and privacy by design, consent and interoperability as core principles.[13] These frameworks make data architecture, consent flows, access controls and governance material design considerations rather than matters that can be deferred to a privacy notice.

In the EU, the General Data Protection Regulation treats data concerning health as a special category of personal data and imposes requirements concerning lawful processing, transparency, purpose limitation, data minimisation, security and data-subject rights.[14] In the US, the Health Insurance Portability and Accountability Act does not apply to every consumer health application. US Department of Health and Human Services guidance explains that information received at an individual's direction by an app that is neither a covered entity nor a business associate is generally no longer protected by the HIPAA Rules once received by that app.[15] Other rules may nevertheless apply. The Federal Trade Commission's Health Breach Notification Rule covers qualifying vendors of personal health records and related entities, including health apps within its scope, and requires notification following certain breaches of unsecured identifiable health information.[16]

Cybersecurity creates a parallel safety and business risk. The FDA's February 2026 guidance addresses cybersecurity design, labelling and premarket documentation for devices with cybersecurity risk and incorporates statutory considerations for cyber devices.[17] For connected clinical products, secure authentication, access control, update mechanisms, vulnerability management and incident-response planning may therefore influence both regulatory readiness and institutional procurement.

Artificial intelligence and accountability

AI can intensify existing regulatory questions because performance may depend on training data, deployment population, clinical workflow and software version. The EU Artificial Intelligence Act establishes a risk-based

framework that interacts with sectoral product regulation; qualifying AI systems used as safety components of regulated products can fall within the high-risk regime.[18] The implementation timetable has been amended, and as of August 2026 the European Commission states that high-risk rules for AI embedded in regulated products, including medical devices, are scheduled to apply from August 2, 2028.[19] This timeline should be rechecked when planning a future EU launch because implementation measures may continue to evolve.

Accountability also extends beyond authorisation. Digital tools may distribute decisions among clinicians, developers, healthcare organisations and automated systems. Open-access analysis of malpractice risks has identified concerns involving virtual assessment, interpretation of novel digital data, automation and continuity of care.[20] It would be inappropriate to assume that an algorithm automatically transfers responsibility away from a clinician or that a developer is responsible for every downstream clinical decision. The relevant duties depend on product design, claims, professional standards, contracts and applicable law. Clear intended-use statements, known limitations, user training, auditability and escalation pathways can reduce ambiguity, although they do not eliminate legal responsibility.

Reimbursement, interoperability and scale-up

Regulatory authorisation is not equivalent to adoption. Payers and healthcare organisations may require evidence of clinical value, workflow compatibility, budget impact or health-economic benefit before they purchase or reimburse a digital product. Comparative work on digital-health access and reimbursement has shown substantial variation in pathways and evidence expectations across jurisdictions.[21]

Interoperability is equally important for products that must exchange data with electronic health records, laboratories, devices or national digital infrastructure. Expert work on digital-health scale-up has identified regulation, liability, funding, reimbursement, integration and interoperability among the factors that can enable or obstruct wider implementation.[22] A 2025 scoping review of telemonitoring systems found continuing heterogeneity in interoperability approaches despite the availability of standards such as HL7 FHIR.[23]

The EU European Health Data Space Regulation creates a framework for primary and secondary use of electronic health data and for aspects of electronic health record systems.[24] Its implementation is staged: the Regulation entered into force in March 2025, key implementing acts are due by March 2027, and major application milestones begin from March 2029 with further phases thereafter.[25] For entrepreneurs, these developments support a practical distinction between market authorisation and market readiness. Table II and Figure 2 summarise a compliance-by-design approach that integrates regulatory and commercial questions throughout development.

Table II. Compliance-by-design questions across the digital health venture lifecycle

Venture stage	Key question	Principal risk if deferred	Practical response
Problem definition	What clinical or health-system need is being addressed?	Weak value proposition or inappropriate clinical claim	Define intended users, setting, problem and measurable value
Product design	Does the intended function meet a medical-device definition?	Unexpected classification or redesign	Map intended purpose and target jurisdictions before locking claims
Evidence planning	What evidence supports safety, performance and clinical value?	Prototype data may not support the final claim	Align validation population, comparator, outcomes and workflow with intended use
Data architecture	What personal/health data are collected, why and under what authority?	Privacy, consent or contractual failures	Apply minimisation, lawful processing, governance and

			access controls by design
Security engineering	Could a vulnerability affect confidentiality, integrity, availability or patient safety?	Late re-engineering and procurement barriers	Build secure authentication, update and vulnerability-management processes
Market entry	What authorisation, certification or licensing pathway applies?	Delayed launch or incomplete submission	Prepare jurisdiction-specific quality and regulatory documentation
Adoption and scale	How will the product be paid for and integrated?	Authorised product fails to achieve routine use	Plan reimbursement, procurement, interoperability and workflow implementation
Post-market phase	How will incidents, performance drift and software changes be managed?	Uncontrolled updates or unrecognised safety problems	Maintain surveillance, change control, incident response and periodic evidence review

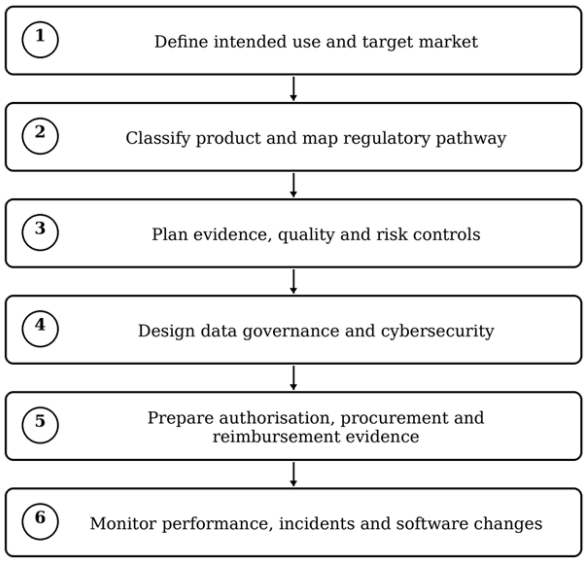

Figure 2. Compliance-by-design framework linking product development with regulatory and market readiness. The sequence is illustrative rather than a legal decision tree; specific obligations depend on intended use, risk classification, business relationships and jurisdiction. Original schematic prepared for this review; no external graphical material was reproduced.

Implications for digital health entrepreneurship in India

India offers a large and increasingly connected digital-health environment, but a single label such as "health-tech startup" does not determine the applicable legal framework. A company may simultaneously need to assess whether its software is a medical device, how personal data are processed, whether it participates in the Ayushman Bharat Digital Mission ecosystem, and what contractual or professional rules apply to the service model.[6,7,11-13]

The 2026 CDSCO guidance is particularly relevant because it provides a more explicit reference for medical device software under the Medical Devices Rules.[7] The guidance does not create a new category for every health-related application; its scope turns on medical purpose and the device definition. Similarly, the DPDP framework should be read according to its phased commencement rather than described as a single fully effective event.[11,12] For ventures that intend to expand internationally, differences between India, the US and the EU make early jurisdictional mapping useful. A domestic evidence package or privacy architecture may need adaptation before use in another market.

Discussion

This review indicates that the principal regulatory challenge in digital health entrepreneurship is not a single approval requirement but the interaction of multiple decisions across the product lifecycle. Intended purpose can determine whether device regulation applies; clinical claims shape evidence needs; data flows influence privacy and security duties; software changes affect validation and post-market responsibilities; and reimbursement and interoperability influence whether an authorised product is actually adopted. These domains are interconnected, so treating compliance as a late-stage legal review can expose a venture to redesign, delayed evidence generation or a business model that is difficult to implement.

The cross-jurisdictional comparison also shows convergence in broad objectives but divergence in legal structure. India, the US and the EU all use risk-oriented concepts for medical software, yet their pathways, data-protection rules and AI requirements are not interchangeable. The US combines sector-specific health privacy with broader consumer protection; the EU combines medical-device rules, general data protection and an emerging horizontal AI framework; and India is integrating medical-device regulation, a phased personal-data regime and national digital-health infrastructure. This fragmentation is relevant to startups because international scaling can require more than translation of documentation.

The review has strengths in its use of openly accessible peer-reviewed evidence and current official regulatory sources, including developments through August 2026. It also has limitations. It is a narrative review and does not provide exhaustive database coverage or quantitative estimates. Only three major regulatory settings are examined in depth, and legal interpretation may differ according to the exact product, contractual relationships and national implementation. Rapidly changing digital-health rules also mean that dates and guidance should be rechecked immediately before a regulatory submission or market launch.

A proportionate lifecycle approach is therefore preferable to either regulatory avoidance or excessive compliance activity at the prototype stage. Entrepreneurs can identify high-impact questions early - intended purpose, target jurisdiction, evidence plan, data governance, cybersecurity, reimbursement and integration - while refining detailed documentation as the product matures. Regulation may create cost and delay, but clear and proportionate requirements can also support safety, accountability and trust. The practical objective is not to remove regulation from innovation, but to align product development with the regulatory conditions under which the technology will be used.

Conclusion

Digital health ventures move through a market pathway in which clinical, technical, legal and commercial decisions are closely linked. Medical-device classification, evidence generation, data protection, cybersecurity, AI governance, liability, reimbursement and interoperability can each affect whether an innovation progresses from prototype to routine use. No single regulatory strategy is appropriate for every digital health product or jurisdiction. However, the reviewed evidence supports early, risk-proportionate integration of regulatory planning with product and business development. Such an approach may reduce avoidable redesign and improve market readiness while maintaining appropriate attention to patient safety, accountability and trust.

Declarations

- **Financial support & sponsorship:** Nil.
- **Conflicts of interest:** None declared.
- **Ethical approval:** Not applicable.
- **Data sharing statement:** Not applicable. No primary research dataset was generated or analysed.
- **Disclaimer:** This article provides a scholarly overview of regulatory issues and does not constitute product-specific legal advice.
- **Acknowledgment:** None.
- **Author Contributions:** All authors contributed to the conception and design of the study, data collection, analysis and interpretation of the findings, preparation and critical revision of the manuscript. All authors read and approved the final manuscript.

References:

[1] World Health Organization. Global strategy on digital health 2020-2027. Geneva: World Health Organization; 2025. ISBN 978-92-4-011687-0. Available from: https://www.who.int/publications/i/item/9789240116870, accessed on August 27, 2026.

[2] Weimar SN, Martjan RS, Terzidis O. Conceptualizing the landscape of digital health entrepreneurship: a systematic review and research agenda. Management Review Quarterly. 2025;75:1619-67. doi: 10.1007/s11301-024-00417-0.

[3] Largent EA, Karlawish J, Wexler A. From an idea to the marketplace: identifying and addressing ethical and regulatory considerations across the digital health product-development lifecycle. BMC Digit Health. 2024;2:41. doi: 10.1186/s44247-024-00098-5.

[4] Chakraborty I, Edirippulige S, Ilavarasan PV. The role of telehealth startups in healthcare service delivery: a systematic review. Int J Med Inform. 2023;174:105048. doi: 10.1016/j.ijmedinf.2023.105048.

[5] US Food and Drug Administration. Digital Health Policy Navigator [Internet]. Silver Spring (MD): US Food and Drug Administration. Available from: https://www.fda.gov/medical-devices/digital-health-center-excellence/digital-health-policy-navigator, accessed on August 27, 2026.

[6] Ministry of Health and Family Welfare, Government of India. Medical Devices Rules, 2017. G.S.R. 78(E), January 31, 2017. New Delhi: Government of India; 2017. Available from: https://cdsco.gov.in/opencms/resources/UploadCDSCOWeb/2022/m_device/Medical%20Devices%20Rules%2C%202017.pdf, accessed on August 27, 2026.

[7] Central Drugs Standard Control Organisation. Guidance document on Medical Device Software under MDR-2017. Doc. No. CDSCO/MD/GD/MDSW/01/2026. New Delhi: Directorate General of Health Services, Ministry of Health and Family Welfare, Government of India; 2026. Available from: https://www.cdsco.gov.in/opencms/opencms/en/Medical-Device-Diagnostics/Medical-Device-Diagnostics/, accessed on August 27, 2026.

[8] European Parliament, Council of the European Union. Regulation (EU) 2017/745 of April 5, 2017 on medical devices. Off J Eur Union. 2017;L117:1-175. Available from: https://eur-lex.europa.eu/eli/reg/2017/745/oj, accessed on August 27, 2026.

[9] Carolan JE, McGonigle J, Dennis A, Lorgelly P, Banerjee A. Technology-enabled, evidence-driven, and patient-centered: the way forward for regulating software as a medical device. JMIR Med Inform. 2022;10:e34038. doi: 10.2196/34038.

[10] US Food and Drug Administration. Marketing Submission Recommendations for a Predetermined Change Control Plan for Artificial Intelligence-Enabled Device Software Functions: Guidance for Industry and Food and Drug Administration Staff [Internet]. Silver Spring (MD): US Food and Drug Administration; 2025. Available from: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/marketing-submission-recommendations-predetermined-change-control-plan-artificial-intelligence, accessed on August 27, 2026.

[11] Government of India. The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023). New Delhi: Ministry of Law and Justice; 2023. Available from: https://www.indiacode.nic.in/indiacode/handle/123456789/22037, accessed on August 27, 2026.

[12] Ministry of Electronics and Information Technology, Government of India. Digital Personal Data Protection Rules, 2025 [Internet]. New Delhi: Ministry of Electronics and Information Technology; 2025. Available from: https://www.meity.gov.in/documents/act-and-policies/digital-personal-data-protection-rules-2025-gDOxUjMtQWa, accessed on August 27, 2026.

[13] National Health Authority. Health Data Management Policy. New Delhi: Ministry of Health and Family Welfare, Government of India; 2020. Available from: https://abdm.gov.in/static/media/health_management_policy_bac9429a79.80f74bc3e039c00acd4f.pdf, accessed on August 27, 2026.

[14] European Parliament, Council of the European Union. Regulation (EU) 2016/679 of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Off J Eur Union. 2016;L119:1-88. Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj, accessed on August 27, 2026.

[15] US Department of Health and Human Services, Office for Civil Rights. The access right, health apps, & APIs [Internet]. Washington (DC): US Department of Health and Human Services; 2025. Available from: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access-right-health-apps-apis/index.html, accessed on August 27, 2026.

[16] Federal Trade Commission. Health Breach Notification Rule. 16 CFR Part 318 [Internet]. Washington (DC): Federal Trade Commission; 2024. Available from: https://www.ftc.gov/legal-library/browse/rules/health-breach-notification-rule, accessed on August 27, 2026.

[17] US Food and Drug Administration. Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions: Guidance for Industry and Food and Drug Administration Staff [Internet]. Silver Spring (MD): US Food and Drug Administration; 2026. Available from: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-management-system-considerations-and-content-premarket, accessed on August 27, 2026.

[18] European Parliament, Council of the European Union. Regulation (EU) 2024/1689 of June 13, 2024 laying down harmonised rules on artificial intelligence. Off J Eur Union. 2024;2024/1689. Available from: https://eur-lex.europa.eu/eli/reg/2024/1689/oj, accessed on August 27, 2026.

[19] European Commission. Navigating the AI Act [Internet]. Brussels: European Commission; 2026. Available from: https://digital-strategy.ec.europa.eu/en/faqs/navigating-ai-act, accessed on August 27, 2026.

[20] Rowland SP, Fitzgerald JE, Lungren M, Lee EH, Harned Z, McGregor AH. Digital health technology-specific risks for medical malpractice liability. NPJ Digit Med. 2022;5:157. doi: 10.1038/s41746-022-00698-3.

[21] Mantovani A, Leopaldi C, Nighswander CM, Di Bidino R. Access and reimbursement pathways for digital health solutions and in vitro diagnostic devices: current scenario and challenges. Front Med Technol. 2023;5:1101476. doi: 10.3389/fmedt.2023.1101476.

[22] Schlieter H, Marsch LA, Whitehouse D, Otto L, Londral AR, Teepe GW, et al. Scale-up of digital innovations in health care: expert commentary on enablers and barriers. J Med Internet Res. 2022;24:e24582. doi: 10.2196/24582.

[23] Martins D, Lewerenz S, Carmo A, Martins H. Interoperability of telemonitoring data in digital health solutions: a scoping review. Front Digit Health. 2025;7:1502260. doi: 10.3389/fdgth.2025.1502260.

[24] European Parliament, Council of the European Union. Regulation (EU) 2025/327 of February 11, 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847. Off J Eur Union. 2025;2025/327. Available from: https://eur-lex.europa.eu/eli/reg/2025/327/oj, accessed on August 27, 2026.

[25] European Commission. European Health Data Space Regulation (EHDS) [Internet]. Brussels: European Commission; 2026. Available from: https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en, accessed on August 27, 2026.