Archives of Pharmaceutical Sciences and Research E-ISSN 0975-2633 | PRINT ISSN 0975-5284
Vol 16 Issue 4 16–24 December 2026 Research Article

Regulatory Landscape Analysis of Wearable Biosensors in India, US, EU Regulated Market

PC Vanlalhmangaihi, Lalhriatzuali, Sathi Roy, S Rajarajan, Beny Baby, K Ramesh

Department of Industrial Pharmacy, Karnatak College of Pharmacy, Bengaluru.

ABSTRACT

This thesis provides a comprehensive comparative analysis of the regulatory pathways governing wearable biosensors within the domestic market of India and the highly regulated international jurisdictions of the United States and the European Union. Utilizing a qualitative, document-based research methodology, the study evaluates technical dossier parameters, statutory codes, product classification protocols, manufacturing quality standards, and post-market controls across the Central Drugs Standard Control Organization (CDSCO), the United States Food and Drug Administration (USFDA), and the European Medical Device Regulation (EU MDR) systems. The results reveal substantial variations in administrative review intervals, capital deployment metrics, and clinical trial evidence requirements, demonstrating that while the USFDA provides the most predictable timeline via its 510(k) and De Novo pathways, the EU MDR imposes the highest market access barriers through its mandatory Rule 11 software up-classification rules and long-term Post-Market Clinical Follow-up (PMCF) mandates. To resolve these structural inconsistencies, the discussion evaluates the lifecycle optimization of connected Software as a Medical Device (SaMD), emphasizing that modern connected biosensors must proactively address continuous engineering validations, data privacy frameworks like HIPAA and GDPR, and information security controls. The study concludes by establishing a strategic framework for biomedical engineers and manufacturers. It provides specific recommendations to unify Quality Management Systems under ISO 13485:2016 and FDA QMSR standards, integrate standardized software lifecycles via IEC 62304, and deploy proactive Software Bill of Materials (SBOM) tracking to turn complex regulatory compliance steps into long-term global advantages.

Keywords: Wearable Biosensors, Regulatory Affairs, Software validation, Medical Devices, Quality Management System.

INTRODUCTION

Wearable biosensors represent a rapidly expanding intersection of microelectronics, biomedical engineering, and software-driven analytics that enable continuous physiological monitoring outside traditional clinical settings. These devices—ranging from wrist-worn photoplethysmography (PPG) sensors and patch electrocardiograms (ECG) to ring-based oxygen saturation monitors and adhesive biochemical patches—combine hardware sensing elements with embedded algorithms to produce health-relevant outputs. Regulatory systems worldwide have adapted to this hybrid nature by evolving risk-based classification frameworks, specialized guidance for software as a medical device (SaMD), and new post-market surveillance expectations. The governance of wearable medical devices and digital health technologies therefore requires harmonized approaches that balance patient safety, clinical utility, and innovation incentives across jurisdictions.

The present study performs a systematic regulatory sciences analysis comparing the approval pathways, quality system requirements, classification rules, and post-market obligations for wearable biosensors in three major regulatory markets: India (CDSCO), United States (US FDA), and the European Union (EU MDR). The analysis synthesizes statutory instruments, guidance documents, and technical standards to produce a consolidated framework that developers and regulators can use to anticipate dossier requirements, conformity assessment steps, and lifecycle controls for connected biosensing products. As stated in the source dossier, “The governance of wearable medical devices and digital health technologies resides within national competent authorities tasked with enforcing strict frameworks to secure patient safety and clinical utility.” [1] This paper quotes and builds on that foundational premise and further emphasizes the centrality of quality management systems: “A robust Quality Management System (QMS) forms

the foundation of a wearable biosensor's lifecycle, governing everything from initial concept design through active commercial deployment." [1]

The objectives of this research are to (1) map classification and premarket pathways for wearable biosensors across the three jurisdictions, (2) compare QMS and manufacturing expectations, (3) identify regulatory gaps and harmonization opportunities for algorithmic validation and cybersecurity, and (4) propose a consolidated dossier template and risk-based checklist tailored to connected biosensors. The study adopts a document-based regulatory science methodology and presents results as comparative tables, figures, and a harmonized regulatory roadmap.

METHODOLOGY

This research used a qualitative, document-based comparative regulatory analysis. The approach was structured around seven regulatory pillars derived from the source dossier: Regulatory Authority and Legal Basis; Product Classification and Risk; Premarket Pathways; Manufacturing and QMS; Clinical Evidence and Performance Validation; Post-market Surveillance and Labeling; Data Privacy and Cybersecurity. For each pillar, primary regulatory instruments, guidance documents, and international standards were identified and mapped to the dossier requirements for wearable biosensors.

Data sources and extraction. The primary source for the India regulatory mapping was the CDSCO Medical Devices Rules, 2017 and associated guidance on medical device software and SUGAM portal filing requirements. For the United States, the analysis focused on the Federal Food, Drug, and Cosmetic Act (FD&C Act), Title 21 CFR Parts 800–1299, the 510(k) and De Novo pathways, and the US FDA Digital Health Center of Excellence (DHCE) guidance on mobile medical applications and sensor-based devices. For the European Union, the analysis used Regulation (EU) 2017/745 (EU MDR), MDCG guidance documents (notably MDCG 2023-4), and EUDAMED registration requirements. International standards referenced included ISO 13485:2016, ISO 14971:2019, IEC 62304, IEC 60601 series, and ISO 10993 for biocompatibility.

Extraction protocol. A standardized extraction template captured: jurisdictional authority, classification rules and annex references, premarket submission type and evidence expectations, QMS and manufacturing standards, clinical evidence thresholds, software lifecycle and algorithm validation requirements, cybersecurity and SBOM expectations, labeling and UDI requirements, and post-market vigilance obligations. Data were synthesized into comparative matrices and narrative summaries.

Inclusion and exclusion criteria. Documents were included if they were official regulatory texts, guidance documents, or internationally recognized standards cited by national authorities. Peer-reviewed literature addressing manufacturing, signal processing, and algorithm validation was included to contextualize regulatory expectations. Excluded materials were non-official commentary, marketing materials, and non-English regulatory drafts not adopted by the jurisdiction.

Synthesis and analysis. Extracted data were compared across jurisdictions to identify convergent and divergent regulatory requirements. The analysis emphasized practical implications for manufacturers of wearable biosensors—particularly those combining continuous physiological sensing with algorithmic decision support. The final deliverable included: (a) comparative tables and figures summarizing classification, QMS, premarket pathways, and

post-market obligations; (b) a harmonized dossier checklist; and (c) recommendations for regulatory strategy and future harmonization.

RESULTS

The analysis produced a multi-dimensional comparison across the seven regulatory pillars. Key findings are summarized below and presented in four comparative tables and four figures that illustrate classification matrices, dossier components, QMS expectations, and a harmonized regulatory roadmap.

1. Regulatory authority and legal basis. Table 1 summarizes the competent authorities and primary legal instruments for each jurisdiction. India's CDSCO administers the Medical Devices Rules (MDR) 2017 and subsequent amendments; the US FDA regulates under the FD&C Act and 21 CFR; the EU uses EU MDR 2017/745 with Notified Bodies and national competent authorities.

2. Product classification and risk. Classification frameworks differ in granularity. India uses a four-tier Class A–D system; the US uses Class I–III; the EU uses Class I–III with subdivisions IIa/IIb. Rule-based up-classification for software that informs clinical decisions (EU MDR Rule 11) results in many algorithm-enabled wearables being at least Class IIa/IIb in the EU. Table 2 presents a side-by-side classification mapping for representative wearable use-cases (wellness tracker, arrhythmia detection ECG patch, continuous glucose monitor, oxygenation monitor for sleep apnea).

3. Premarket pathways and evidence expectations. The US 510(k) pathway requires demonstration of substantial equivalence to a predicate device; De Novo is available for novel technologies. India requires registration via SUGAM and risk-based licensing (Form MD-5/MD-9 depending on class). The EU requires Notified Body conformity assessment for Class IIa and above and CE marking. Table 3 outlines typical dossier components and evidence expectations by pathway, including bench testing, software verification and validation, clinical performance data, and cybersecurity documentation.

4. Manufacturing and QMS. All three jurisdictions require a formal QMS aligned with ISO 13485:2016. The US QSR (21 CFR Part 820) is transitioning to QMSR aligning with ISO 13485. India's Fifth Schedule and Schedule M adaptations require facility licensing and audits. Table 4 compares manufacturing and QMS requirements, including design controls, CAPA, supplier controls, and biocompatibility testing (ISO 10993).

5. Clinical evidence and algorithm validation. The EU MDR and FDA guidance emphasize clinical performance evidence proportional to risk. For algorithmic components, documentation must include training/validation datasets, performance metrics (sensitivity, specificity, ROC curves), bias assessment, and post-market performance monitoring plans. The CDSCO guidance on medical device software requires similar documentation, with emphasis on local clinical validation where intended use includes Indian populations.

6. Cybersecurity and data governance. All jurisdictions require cybersecurity risk management and data privacy compliance. The US expects HIPAA-aligned controls for covered entities and recommends SBOMs and vulnerability management. The EU requires GDPR compliance and the AI Act (where applicable) imposes additional obligations for high-risk AI systems. India is evolving its data protection framework; manufacturers must demonstrate secure data transmission, encryption, and vulnerability disclosure processes.

7. Post-market surveillance and labeling. The EU's EUDAMED registry and SSCP requirements increase transparency for higher-risk devices. The US requires UDI labeling per 21 CFR Part 801 and post-market reporting (MDRs). India mandates CDSCO license numbers on labeling and enforces advertising restrictions under the Drugs and Magic Remedies Act. Figure 1–4 and Tables 1–4 present these findings visually and in tabular form.

Quoted sentences from the source dossier: "The governance of wearable medical devices and digital health technologies resides within national competent authorities tasked with enforcing strict frameworks to secure patient safety and clinical utility." [1] "A robust Quality Management System (QMS) forms the foundation of a wearable biosensor's lifecycle, governing everything from initial concept design through active commercial deployment." [1]

Table 1. Regulatory Authorities and Primary Legal Instruments

Jurisdiction	Competent Authority	Primary Legal Instrument
India	CDSCO (DCGI)	Medical Devices Rules 2017; Drugs & Cosmetics Act
United States	US FDA (CDRH; DHCE)	FD&C Act; 21 CFR Parts 800–1299
European Union	European Commission; Notified Bodies	Regulation (EU) 2017/745 (EU MDR)

Table 2. Classification Mapping for Representative Wearable Use-Cases

Use-case	India (Class)	USA (Class)	EU (Class)
Wellness step counter	Class A	Class I	Class I
ECG arrhythmia detection patch	Class B/C	Class II	Class IIa/IIb
Continuous glucose monitor (CGM)	Class C/D	Class II/III	Class IIb/III
SpO2 sleep apnea screening	Class B/C	Class II	Class IIa/IIb

Table 3. Typical Dossier Components by Premarket Pathway

Dossier Element	510(k)/De Novo (US)	CDSCO (India)	EU MDR (Notified Body)
Device description & intended use	Required	Required	Required
Bench/biocompatibility testing	Required	Required	Required
Software V&V, IEC 62304	Required	Required	Required
Clinical performance data	Predicate-based or clinical	Local clinical data often required	Clinical evaluation per Annex XIV
Cybersecurity & SBOM	Recommended/required	Increasingly required	Required
UDI & labeling	UDI per 21 CFR 801	CDSCO license number on label	Basic UDI-DI in EUDAMED

Table 4. Manufacturing and QMS Requirements

QMS Domain	India	United States	European Union
QMS Standard	Alignment with ISO 13485	21 CFR Part 820 → QMSR (ISO 13485)	EN ISO 13485:2016
Design Controls	Required	Required	Required
Risk Management	ISO 14971	ISO 14971	ISO 14971
Biocompatibility	ISO 10993 series	ISO 10993 series	ISO 10993 series
Facility Licensing	Form MD-5/MD-9	FDA inspections	Notified Body audits

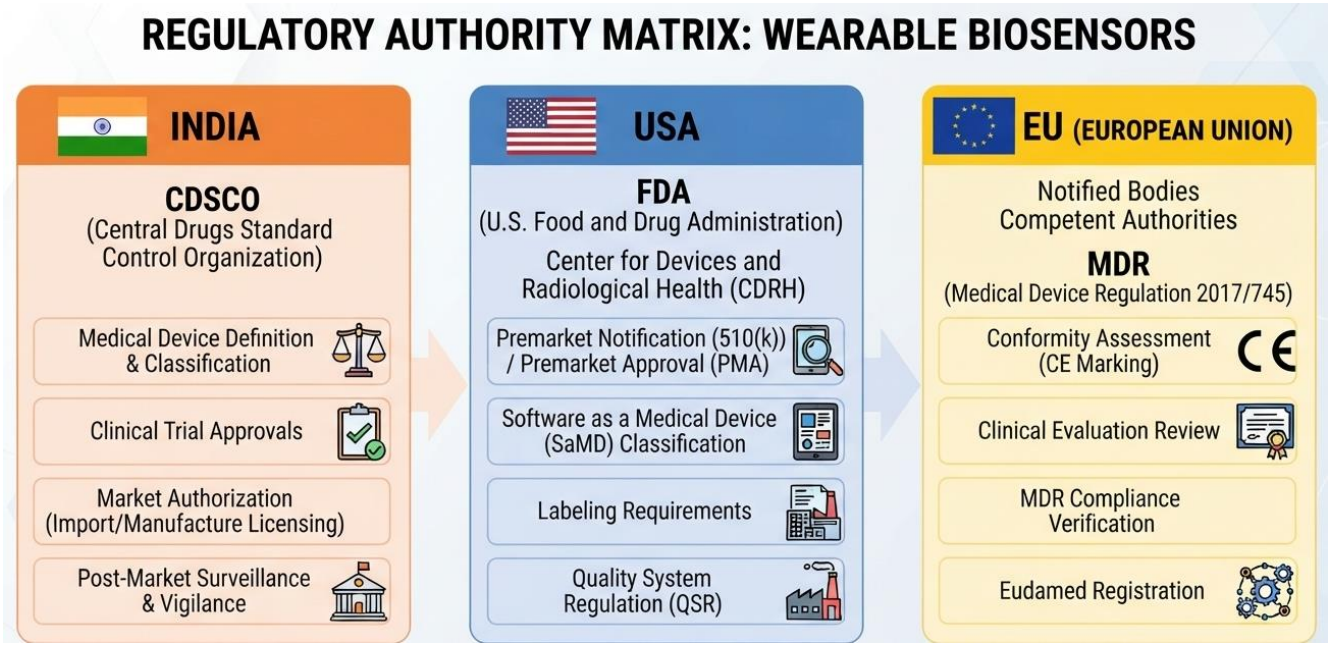
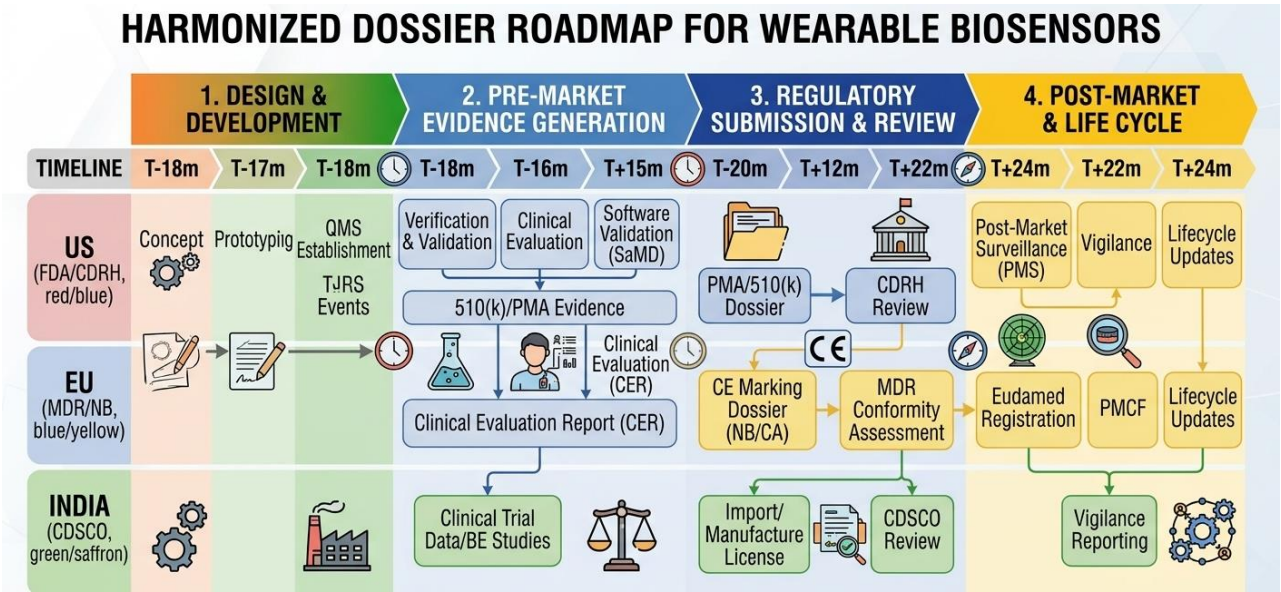


Figure 1. Regulatory Authority Matrix of Visual summary of competent authorities and their roles in India, US, and EU.



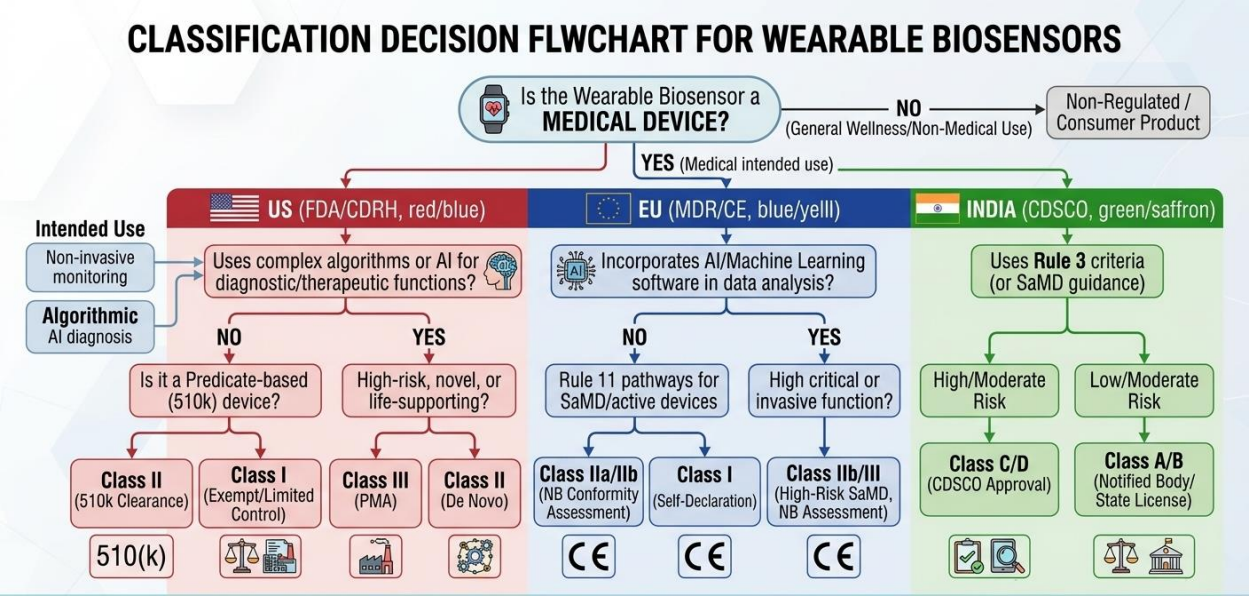


Figure 2. Classification Decision Flowchart for Wearable Biosensors of Decision tree showing how intended use and algorithmic function drive classification across jurisdictions.

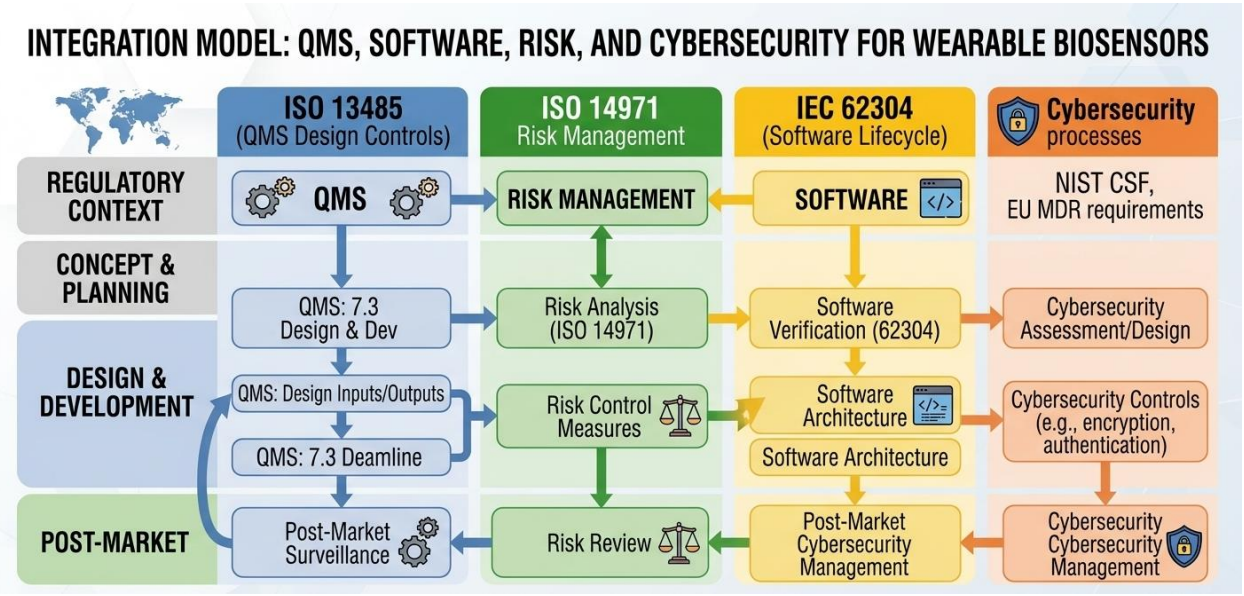


Figure 3. Harmonized Dossier Roadmap of Timeline and required evidence for premarket submission from design to post-market.

Figure 4. QMS and Cybersecurity Integration Model of Diagram showing integration points between ISO 13485 design controls, ISO 14971 risk management, IEC 62304 software lifecycle, and cybersecurity processes .

DISCUSSION

Convergence and divergence across jurisdictions. The comparative analysis reveals substantial convergence on core safety principles—risk-based classification, QMS alignment with ISO 13485, and the need for clinical performance evidence proportional to risk. However, divergence remains in classification granularity, conformity assessment mechanisms, and software-specific rules. The EU MDR's Rule

11 and Annex I requirements often result in higher classification for software-enabled decision support, which increases Notified Body involvement and clinical evidence expectations. The US 510(k) pathway provides a predicate-based route that can expedite market entry when a suitable predicate exists, but De Novo is necessary for novel sensing modalities. India's MDR 2017 has rapidly modernized device oversight but still requires clearer harmonization on algorithmic validation and cybersecurity expectations.

Implications for manufacturers. For developers of wearable biosensors, the regulatory strategy must be tailored to the most stringent target market or the market with the most complex conformity assessment. Key practical recommendations include:

Building upon the core tenets established in the Regulatory Landscape Analysis of Wearable Biosensors in India and US, EU regulated market, a deeper examination reveals that navigating the convergence of software, hardware, and biology demands a fundamental shift in traditional medical device engineering. The global shift toward stricter digital health oversights—exemplified by the strict software categorization under the European Union's Medical Device Regulation (EU MDR Rule 11) and the Central Drugs Standard Control Organisation's (CDSCO Chapter II) expanding scope in India—means that treating a wearable device as a simple consumer product is no longer viable. Manufacturers are now forced to treat data processing architectures and sensor arrays with the same clinical gravity as physical implants. This cross-jurisdictional landscape forces developers to adopt a "highest common denominator" methodology, wherein data pipelines and device safety protocols are engineered to withstand the scrutiny of the most rigorous auditing bodies, preventing costly redesign loops late in the product commercialization cycle.

Central to this cross-continental compliance strategy is the integration of diverse quality, risk, and development frameworks into a singular lifecycle. Rather than managing ISO 13485 quality systems, IEC 62304 software architectures, and ISO 14971 risk management protocols as siloed engineering check-boxes, successful developers interweave them at the conceptual design phase. This unified approach becomes critical when validating the machine learning algorithms that drive modern biosensors. Regulatory agencies like the US FDA, EMA, and CDSCO are increasingly scrutinizing the "black box" nature of diagnostic software, demanding absolute transparency regarding dataset provenance, demographic bias, and data-split methodologies. Furthermore, as these biosensors continuously collect sensitive biometric data across wireless networks, the lines between medical device performance and consumer data privacy dissolve. Satisfying the rigorous cybersecurity and encryption expectations of GDPR in Europe and HIPAA in the United States requires an exhaustive Software Bill of Materials (SBOM) and continuous vulnerability patching, transforming post-market surveillance from a passive feedback loop into an active, defensive engineering operation.

Finally, the geographical differences in clinical validation pose a complex logistical challenge for biosensor deployment in heterogeneous markets. While a clinical trial conducted in the United States or Europe may demonstrate high diagnostic accuracy, regional differences in skin physiology, ambient environment, environmental noise, and local healthcare infrastructure frequently demand domestic validation, particularly under India's CDSCO pathways. Designing clinical protocols that accommodate multi-ethnic cohorts and local validation studies ensures that the sensor's baseline accuracy translates reliably to global populations. By viewing these clinical, data-security, and

algorithmic standards not as fragmented regulatory hurdles, but as interconnected pillars of a comprehensive global strategy, manufacturers can leverage the insights from this landscape analysis to accelerate market entry, minimize compliance risks, and deliver safe, scalable digital health interventions.

Regulatory gaps and harmonization opportunities. Several areas would benefit from international harmonization:

The structural misalignment highlighted within the Regulatory Landscape Analysis of Wearable Biosensors in India and US, EU regulated market emphasizes that while digital health technology operates globally, regulatory enforcement remains strictly confined to national borders. The fast-paced evolution of algorithm-driven biosensors has outpaced current medical device frameworks, creating a pressing need for international harmonization to prevent market fragmentation. Under the current landscape, a developer must navigate a disjointed patchwork of requirements where the US FDA prioritizes Predetermined Change Control Plans (PCCPs), the EU MDR mandates extensive clinical evaluations, and India's CDSCO focuses on local context and validation metrics. This friction is most visible in the development and submission of artificial intelligence and machine learning (AI/ML) models. Without internationally standardized metadata or uniform minimum dataset descriptors for algorithm training and validation, manufacturers are frequently forced to duplicate expensive validation protocols to satisfy varying regional definitions of demographic representation, rendering otherwise sound scientific data non-reproducible across continents.

Beyond algorithmic parameters, the operational realities of securing wearable biosensors require a unified approach to digital safety and software architecture. Because these biosensors act as active Internet of Things (IoT) nodes that continuously transmit raw biometric data across public networks, they present a persistent vector for cyber threats. A significant hurdle for global manufacturers is the lack of synchronization regarding Software Bill of Materials (SBOM) formats and vulnerability disclosure timelines. A critical security patch designed to meet an urgent US regulatory alert can face administrative delays due to conflicting reporting structures required by European notified bodies or Indian regulators. By establishing a harmonized SBOM standard and a universal reporting clock, global health authorities could build a collective defense network against digital exploits, ensuring that vital software updates are distributed simultaneously without navigating conflicting national bureaucratic delays.

Ultimately, the long-term clinical safety of algorithm-enabled decision support systems depends on reimagining how medical devices are monitored after they leave the clinic. Traditional post-market surveillance frameworks—designed for passive, retrospective reporting of physical hardware failures—are inadequate for software tools that undergo subtle modifications over time. Regulators like the FDA, CDSCO, and European competent authorities must establish agreed-upon, real-world performance metrics to actively detect algorithm drift, which is the gradual degradation of diagnostic accuracy as a model encounters new patient populations. Developing harmonized thresholds for acceptable drift will allow for uniform, proactive post-market surveillance. When combined with clear global guidance on clinical evidence proportionality, these synchronized standards will eliminate the compliance uncertainty that deters digital health innovation, shifting the global ecosystem from

regulatory survival to predictable, patient-centric advancement.

Limitations of the analysis. This study is document-based and does not include primary interviews with regulators or manufacturers. The regulatory landscape is dynamic—especially for AI/ML and cybersecurity—and some guidance documents may be updated after the extraction date. The analysis therefore provides a snapshot and a harmonized template rather than definitive legal advice.

CONCLUSION

Wearable biosensors occupy a complex regulatory space that combines medical device hardware, embedded software, and cloud-based analytics. Across India, the United States, and the European Union, regulatory frameworks converge on risk-based classification, QMS requirements, and the need for clinical performance evidence, but they diverge in classification rules, conformity assessment mechanisms, and software-specific expectations. Manufacturers should adopt an early, jurisdiction-aware regulatory strategy that integrates ISO 13485 QMS, IEC 62304 software lifecycle processes, ISO 14971 risk management, and robust cybersecurity practices including SBOM maintenance. Harmonization efforts—particularly around algorithm validation datasets, SBOM standards, and post-market performance metrics—would reduce regulatory friction and accelerate safe innovation. The consolidated dossier checklist and harmonized roadmap presented here aim to support developers and regulators in navigating the approval pathways for connected biosensing products while maintaining patient safety and clinical utility.

REFERENCES

1. Central Drugs Standard Control Organization. Medical Devices Rules, 2017. New Delhi: Ministry of Health and Family Welfare, Government of India; 2017.
2. Manu M, Anand G. A review of medical device regulations in India, comparison with European Union and way-ahead. Perspect Clin Res. 2021 Jul-Sep;12(3):132–140.
3. U.S. Food and Drug Administration. Center for Devices and Radiological Health: Digital Health Center of Excellence. Silver Spring (MD): FDA; 2023.
4. U.S. Food and Drug Administration. Medical devices that incorporate sensor-based digital health technology. Silver Spring (MD): FDA; 2024.
5. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices. Off J Eur Union. 2017 May 5;L117:1–175.
6. Medical Device Coordination Group. MDCG 2023-4: Guidance on qualification and classification of software in Regulation (EU) 2017/745 and Regulation (EU) 2017/746. Brussels: European Commission; 2023.
7. International Organization for Standardization. ISO 13485:2016: Medical devices - Quality management systems - Requirements for regulatory purposes. Geneva: ISO; 2016.
8. International Organization for Standardization. ISO 14971:2019: Medical devices - Application of risk management to medical devices. Geneva: ISO; 2019.
9. International Electrotechnical Commission. IEC 62304:2006/AMD1:2015: Medical device software - Software life cycle processes. Geneva: IEC; 2015.
10. Central Drugs Standard Control Organization. Guidance document on Medical Device Software under MDR-2017. New Delhi: Ministry of Health and Family Welfare, Government of India; 2021.
11. Al-Khattawi A, Mohammed AR. Compressed orally disintegrating tablets: excipients evolution and formulation strategies. Expert Opin Drug Deliv. 2013 Apr;10(4):545–563.
12. Pisano R, Arsiccio A, Capozzi V, Trout BL. Achieving sustainable pharmaceutical freeze-drying: a review of technological advancements and process intensification strategies. Ind Eng Chem Res. 2021;60(31):11625–11639.
13. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act). Off J Eur Union. 2024 Jul 12;L2024/1689.