Risk Management and Healthcare Policy

Dovepress
Taylor & Francis Group

Open Access Full Text Article

REVIEW

Privacy, Security & Governance Frameworks for AI-Powered Wearable Internet of Health Things in Elderly Care: A Comprehensive Review

Dhika Dharmansyah[1,2], Laili Rahayuwati[3], Iqbal Pramukti[3], Kuswandewi Mutyara[4]

[1]Doctoral Program in Medicine, Faculty of Medicine, Universitas Padjadjaran, Sumedang, West Java, Indonesia; [2]Department of Nursing, Faculty of Sport and Health Education, Universitas Pendidikan Indonesia, Bandung, West Java, Indonesia; [3]Department of Community Health Nursing, Faculty of Nursing, Universitas Padjadjaran, Sumedang, West Java, Indonesia; [4]Department of Public Health, Faculty of Medicine, Universitas Padjadjaran, Sumedang, West Java, Indonesia

Correspondence: Dhika Dharmansyah, Doctoral Program in Medicine, Faculty of Medicine, Universitas Padjadjaran, Sumedang, West Java, Indonesia, Email dhika23001@mail.unpad.ac.id

Video abstract

Point your SmartPhone at the code above. If you have a QR code reader the video abstract will appear. Or use: https://youtu.be/JqQJagBVLzQ
Access transcript: https://www.dovepress.com/article/video_transcript/606165

Abstract: The global aging population is expanding at an unprecedented rate, with projections indicating that 1.4 billion people will be aged 60 years or older by 2030 and 2.1 billion by 2050, placing immense pressure on healthcare systems worldwide. Artificial intelligence (AI)-powered wearable Internet of Health Things (IoHT) devices — including smartwatches, biosensors, and continuous health monitors — have emerged as transformative tools for real-time elderly health monitoring, fall detection, and predictive analytics. However, the massive collection of sensitive biometric data by these devices raises critical concerns regarding privacy, security, and governance that remain insufficiently addressed, particularly for elderly populations. This comprehensive review synthesizes evidence from 333 peer-reviewed articles published between 2018 and 2025 cross PubMed, Scopus, Web of Science, IEEE Xplore, and Google Scholar to identify, analyze, and compare governance frameworks for AI-powered wearable IoHT in elderly care. The analysis reveals significant regulatory fragmentation across jurisdictions: while the European Union's General Data Protection Regulation (GDPR) and AI Act provide the most comprehensive rights-based framework, the United States relies on a patchwork of sector-specific regulations with notable gaps for consumer wearables, and Asia-Pacific nations exhibit highly variable approaches ranging from mature (Singapore, Japan) to nascent (Indonesia, Malaysia). Elderly-specific provisions remain conspicuously absent across all regulatory regimes examined. This review proposes a novel five-layer integrative governance framework — the first to unify technical security, privacy protection, ethical AI governance, regulatory compliance, and person-centered governance specifically designed for elderly care contexts. The framework addresses unique vulnerabilities associated with cognitive decline, reduced digital literacy, and caregiver dependency. Findings underscore the urgent need for harmonized, age-sensitive regulatory approaches and privacy-preserving technologies such as federated learning and differential privacy to ensure that AI-powered wearable IoHT fulfills its promise of enhancing elderly healthcare without compromising dignity, autonomy, or data security.

Plain Language Summary: Wearable health devices — such as smartwatches and fitness trackers powered by artificial intelligence — are increasingly used to monitor the health of older adults, tracking heart rate, blood oxygen, physical activity, and even detecting falls. While these devices can significantly improve care for elderly people, they also collect highly sensitive personal health data continuously, raising important questions about who can access this data, how it is protected, and what rules govern its use. This review examined 333 research studies to understand how different countries regulate the privacy and security of health data from these wearable devices, with a specific focus on elderly users. The findings show that no country currently has regulations specifically designed to protect older adults who use AI-powered health wearables. Older people face unique challenges — including memory difficulties, lower familiarity with technology, and reliance on caregivers — that make standard data protection rules insufficient. A new comprehensive framework is proposed to guide governments, device manufacturers, healthcare providers, and caregivers in protecting elderly users while enabling the benefits of wearable health monitoring technology.

https://doi.org/10.2147/RMHP.S606165
Received: 1 March 2026
Accepted: 15 April 2026
Published: 23 April 2026

Keywords: internet of health things, IoHT, wearable AI, privacy governance, elderly care, data security, regulatory framework, risk management

Introduction

Global Aging and the Rise of Wearable IoHT

Respiratory infectious diseases, chronic conditions, and age-related health deterioration collectively represent the most pressing challenges for global health systems contending with rapidly aging populations.[1] The World Health Organization projects that the number of people aged 60 and older will increase from 1.1 billion in 2023 to 1.4 billion by 2030, with two-thirds of this population residing in low- and middle-income countries by 2050.[1,2] Japan already leads globally with approximately 30% of its population aged 65 and older, while the European Union reports that more than one-fifth (22.0%) of its population exceeded 65 years as of January 2025.[3,4] This demographic shift demands innovative healthcare delivery models that extend beyond traditional facility-based care.

The Internet of Health Things (IoHT) — the interconnected ecosystem of medical devices, sensors, and software facilitating health data exchange — has emerged as a promising solution. The global Internet of Medical Things (IoMT) market, valued at approximately $100 billion in 2024, is projected to exceed $257 billion by 2030, driven by rapid advances in wearable sensor technologies.[5,6] These devices — ranging from smartwatches and fitness trackers to specialized medical wearables — monitor vital health metrics such as heart rate, blood pressure, oxygen saturation, glucose levels, and movement patterns in real time, enabling proactive health management and timely interventions.[5,7]

While IoHT and the closely related Internet of Medical Things (IoMT) are sometimes used interchangeably in the literature, IoHT is adopted throughout this review as the primary term to emphasize the broader health-oriented ecosystem encompassing wellness monitoring and preventive care, whereas IoMT more narrowly denotes clinical and medical device applications. Where cited studies use the term IoMT, this terminology is preserved to maintain fidelity to the original source.

AI Integration in Wearable IoHT for Elderly Care

The integration of artificial intelligence and machine learning into wearable bioelectronics is revolutionizing digital healthcare by enabling personalized, data-driven medical solutions.[8] AI-powered wearables facilitate continuous monitoring, anomaly detection, predictive analytics for fall prevention and chronic disease exacerbation, and personalized health recommendations specifically beneficial for elderly populations.[8,9] Recent applications include AI-driven multimodal smart home platforms for post-stroke rehabilitation, federated learning frameworks for elderly healthcare using edge-IoMT architectures, and generative adversarial network-integrated IoT systems for adaptive personalized elderly care.[10–12] These technologies collect massive volumes of sensitive biometric data — heart rate variability, gait patterns, sleep quality, glucose fluctuations, and cognitive function indicators — and process them through increasingly sophisticated AI algorithms to generate clinical insights.[13]

Privacy, Security, and Governance Challenges

The explosive growth of AI-powered wearable IoHT introduces profound privacy and security risks. Healthcare data breaches remain the costliest of any industry, averaging $7.42 million per incident in 2025, with the average breach lifecycle extending to 279 days before detection and containment.[14,15] Medical records command a 10 × premium over credit card data on dark markets ($260–$310 versus $30–$50 per record), underscoring the economic incentives driving cyber threats against health data repositories.[16] In 2024 alone, approximately 275–276 million patient records were compromised in the United States, affecting over 80% of the population.[16,17]

Wearable IoHT devices present unique governance challenges. Consumer wearables frequently operate outside the regulatory perimeter of traditional health data protection frameworks such as the Health Insurance Portability and Accountability Act (HIPAA), which applies only to covered entities.[13] The European Union's AI Act, which entered into force in August 2024, classifies AI systems used for medical purposes — including biometric and health-monitoring

AI in wearable devices — as "high-risk", imposing stringent requirements for data quality, transparency, human oversight, and risk management that extend beyond existing medical device regulations.[18,19] Under the General Data Protection Regulation (GDPR), wearable health data qualifies as special category data under Article 9, requiring explicit consent and enhanced protection, yet the "always-on" nature of wearables poses challenges by increasing the risk of over-collection and complicating meaningful consent.[20] This fragmented regulatory landscape creates compliance complexity for multinational manufacturers and governance gaps that disproportionately affect vulnerable populations.

Research Gap and Objectives

Despite growing recognition of privacy and security challenges in IoMT systems, existing reviews have predominantly focused on technical security frameworks without integrating governance, ethical, and policy dimensions.[21] A scoping review of IoMT security frameworks identified 1341 articles and analyzed frameworks from 2018 to 2023 but concentrated on technical risk assessment rather than cross-jurisdictional regulatory comparison.[21] The SPAU-IoT Framework comprising 27 criteria across four dimensions evaluated security and privacy for older adults but found that fewer than 50% of studies addressed accessibility or usability — two critical aspects for elderly populations.[22] Critically, no existing framework integrates AI-specific risks (algorithmic bias, model opacity, data inference) with privacy governance and elderly-specific vulnerabilities (cognitive decline, digital literacy deficits, caregiver dependency) within a unified analytical structure.[13]

This review addresses these gaps with four objectives: (1) identify and analyze existing governance frameworks for AI-powered wearable IoHT; (2) compare regulatory approaches across the European Union, United States, and Asia-Pacific jurisdictions; (3) evaluate AI-specific risks including algorithmic bias, model opacity, and surveillance creep in elderly care contexts; and (4) propose an integrative governance framework that synthesizes technical, ethical, regulatory, and person-centered dimensions to guide policy development, industry practice, and clinical implementation.

Methods

Study Design

This study employed a comprehensive narrative review methodology to synthesize and critically analyze the existing literature on privacy, security, and governance frameworks for AI-powered wearable IoHT in elderly care. The narrative review approach was selected to accommodate the interdisciplinary nature of the topic, which spans technological, regulatory, ethical, and clinical domains that a purely systematic approach would inadequately capture. The review was guided by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses for Scoping Reviews (PRISMA-ScR) guidelines to ensure methodological transparency and reproducibility.[23]

Search Strategy

A structured literature search was conducted across five electronic databases: PubMed/MEDLINE, Scopus, Web of Science, IEEE Xplore, and Google Scholar. The search period spanned January 2018 to December 2025, corresponding to the post-GDPR era and the period of accelerated IoHT development. Search terms combined Boolean operators and were structured as follows:

("Internet of Health Things" *OR* "IoHT" *OR* "Internet of Medical Things" *OR* "IoMT" *OR* "wearable" *OR* "wearable device") *AND* ("privacy" *OR* "security" *OR* "governance" *OR* "regulation" *OR* "data protection") *AND* ("elderly" *OR* "older adults" *OR* "aging" *OR* "geriatric" *OR* "aged care").

Additional targeted searches were conducted for specific regulatory frameworks (GDPR, HIPAA, EU AI Act, PDPA variants), privacy-preserving technologies (federated learning, differential privacy, blockchain), and ethical dimensions (informed consent, algorithmic bias, autonomy) in elderly care contexts.

Inclusion and Exclusion Criteria

Inclusion criteria: (1) Peer-reviewed articles published in English between 2018 and 2025; (2) studies addressing privacy, security, governance, or ethical dimensions of wearable IoT/IoHT/IoMT in healthcare or elderly care contexts; (3) regulatory analyses, policy reviews, and governance framework proposals relevant to health wearable devices; (4) studies evaluating AI/ML applications in elderly health monitoring with privacy or security implications.

Exclusion criteria: (1) Purely technical articles without governance, policy, or privacy dimensions; (2) non-healthcare IoT applications; (3) conference abstracts without full text; (4) articles in languages other than English; (5) duplicate publications across databases.

Screening and Selection

The initial database search yielded 2,987 records across the five databases (PubMed n=47; Scopus n=991; Web of Science n=1,906; IEEE Xplore n=43), with Google Scholar used for supplementary hand-searching. After automated pre-screening removed 140 cross-database duplicates at the export stage, 2,847 records entered the formal identification phase. Subsequent removal of 612 additional duplicates yielded 2,235 unique records, which were screened by title and abstract against inclusion criteria. Of these, 498 full-text articles were assessed for eligibility. Following full-text evaluation, 333 articles met the inclusion criteria and were retained for analysis (Figure 1). Articles were classified into three relevance tiers: Tier 1 (n=235) representing highest relevance with three or more core themes addressed, Tier 2 (n=59) with moderate relevance, and Tier 3 (n=39) providing supplementary evidence.

Data Extraction and Analysis

A structured data extraction matrix was developed to systematically capture: publication metadata, study design, technology type, governance/regulatory frameworks discussed, privacy-preserving mechanisms evaluated, ethical considerations addressed, and elderly-specific provisions identified. Thematic synthesis was employed to organize findings into six analytical domains: (1) Introduction and landscape; (2) Methods; (3) AI-powered wearable IoHT technologies and risks; (4) Comparative governance frameworks; (5) Ethical dimensions; and (6) Integrative framework proposals. Each included article was mapped to one or more sections based on its primary contribution, with 288 articles contributing to the technology landscape, 289 to AI-wearable IoHT analysis, 163 to governance frameworks, 110 to ethical dimensions, and 141 to integrative framework discussions.

AI-Powered Wearable IoHT in Elderly Care: Landscape and Risks

Technologies and Applications

The landscape of AI-powered wearable IoHT devices for elderly care encompasses a diverse array of technologies designed for continuous health monitoring, disease management, and safety assurance. Smartwatches and fitness trackers equipped with photoplethysmographic (PPG) sensors monitor heart rate and blood oxygen saturation, while dedicated electrodermal activity (EDA) sensors measure sympathetic nervous system arousal through changes in skin conductance.[24] Specialized biosensors further enable continuous glucose monitoring, electrocardiogram (ECG) recording, and respiratory pattern analysis.[8] Fall detection systems have evolved from simple accelerometer-based triggers to sophisticated multi-modal platforms utilizing human pose estimation, transformer deep learning models, and frequency-modulated continuous wave radar, achieving sensitivities exceeding 95% while preserving user privacy through local processing.[25,26]

AI integration enables capabilities beyond passive monitoring. Federated learning frameworks such as FEEL (FEderated LEarning Framework for ELderly Healthcare) demonstrate how edge-IoMT architectures can simultaneously address data scarcity, privacy preservation, and personalized healthcare recommendations, achieving F1 scores of 0.86–0.94 across activity monitoring, fall detection, and medical recommendation tasks.[12] Generative adversarial networks integrated with IoT sensors have shown 30% faster detection of risk conditions and 25% faster response times compared with conventional solutions.[11] AI-driven multimodal smart home platforms integrating wearable sensing, ambient monitoring, and adaptive automation — including embedded large language model agents — have increased user satisfaction from 3.9 ± 0.8 to 8.4 ± 0.6 in post-stroke rehabilitation contexts.[10]

Clinical applications in elderly care span multiple domains: cardiac monitoring and arrhythmia detection, diabetes management through continuous glucose monitoring, Alzheimer's disease stage-wise monitoring and assistive technologies, medication adherence through IoMT-enabled smart pill dispensers, and musculoskeletal rehabilitation through digital twin systems.[8,9,27–29] The breadth of these applications underscores both the transformative potential and the scale of sensitive data collection inherent in modern elderly care IoHT ecosystems.

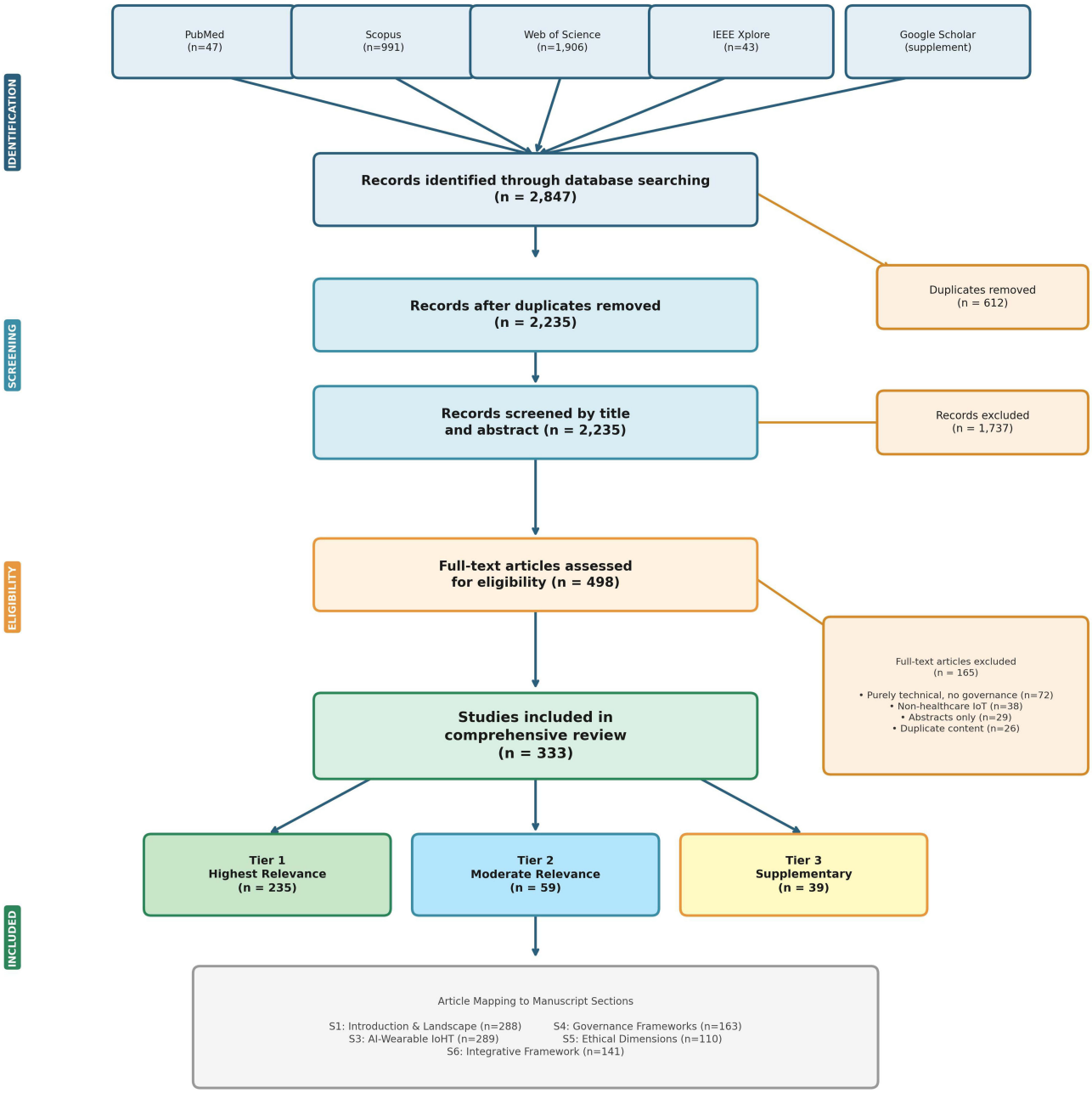

Figure 1 PRISMA Flow Diagram of Study Selection. The diagram illustrates the systematic screening process from initial identification of 2847 records across five databases (PubMed, Scopus, Web of Science, IEEE Xplore, Google Scholar) through deduplication (n=612 removed), title and abstract screening (n=2235), full-text assessment (n=498), to final inclusion of 333 articles classified into three relevance tiers (Tier 1: n=235; Tier 2: n=59; Tier 3: n=39).
Note: The 140-record difference between aggregate database subtotals (n=2,987) and the identified records pool (n=2,847) reflects automated cross-database deduplication performed at the export stage prior to formal PRISMA identification.

AI-Specific Risks in Elderly Wearable IoHT

Algorithmic Bias

AI systems trained on datasets that inadequately represent elderly populations — particularly those with multiple comorbidities, from minority ethnic groups, or residing in low-resource settings — may produce systematically biased recommendations, delayed diagnoses, or inequitable access to healthcare interventions.[30] The heterogeneity of aging processes and the wide variability in physiological baselines among older adults amplify the risk that models validated primarily on younger, healthier populations will perform suboptimally when deployed in geriatric contexts.

https://doi.org/10.2147/RMHP.S606165

Model Opacity

Deep learning models underpinning predictive analytics in wearable IoHT systems frequently operate as "black boxes", generating outputs without transparent reasoning pathways.[13,31] In clinical contexts affecting elderly care decisions — such as fall risk stratification, medication adjustment recommendations, or cognitive decline predictions — the inability to explain AI-generated insights poses challenges for informed consent, clinical trust, and regulatory accountability. Explainable AI (XAI) approaches, including LIME and SHAP, have been integrated into some frameworks to address transparency requirements, but their adoption remains limited in commercial wearable devices.[32]

Data Inference Risks

AI algorithms can infer sensitive information not explicitly collected — cognitive decline trajectories, depression risk profiles, behavioral patterns indicating dementia onset — from seemingly non-sensitive sensor data such as step counts, sleep duration, and movement variability.[33,34] This capability for secondary inference generates privacy risks that exceed the scope of original data collection consent and challenges the principle of data minimization central to GDPR and similar frameworks.

Surveillance Creep

Continuous monitoring through wearable devices, while clinically beneficial, risks transforming healthcare tools into surveillance instruments that threaten the dignity and autonomy of elderly users.[30,35] The boundary between therapeutic monitoring and behavioral surveillance becomes increasingly blurred when caregivers, family members, or institutional managers gain unrestricted access to granular behavioral data.

Security Vulnerabilities Specific to Elderly Users

The SPAU-IoT Framework's analysis reveals that while more than 70% of studies implement authentication and encryption mechanisms, fewer than 50% address accessibility or usability — critical dimensions for elderly users with varying levels of cognitive function, sensory ability, and technical competence.[22] Threat models specific to elderly IoT users encompass exploit vectors including phishing attacks exploiting reduced digital literacy, caregiver exploitation of access privileges, weak-password vulnerabilities due to memory difficulties, and social engineering targeting isolation and trust.[22,34] Studies of IoMT and data privacy in Alzheimer's care have identified recurring vulnerabilities: social engineering, data breaches, weak authentication, poor access control, and insufficient informed consent procedures.[33]

The pervasive data security and privacy concerns constitute a significant market impediment. Healthcare organizations face considerable reputational and financial risks from data breaches, with average costs reaching $7.42 million per incident and the number of healthcare providers reporting losses exceeding $200,000 quadrupling between 2024 and 2025.[14,15] For elderly care specifically, breach consequences extend beyond financial losses to include psychological harm from privacy violations, loss of trust in digital health technologies, and potential exploitation of exposed health information.

Comparative Governance Frameworks Across Jurisdictions

European Union: GDPR and the EU AI Act

The European Union provides the most comprehensive rights-based regulatory framework for AI-powered wearable IoHT. The General Data Protection Regulation (2018) classifies biometric and health data as "special categories of personal data" requiring explicit consent, transparency, and robust user rights including access, correction, and deletion.[20,36] For wearable AI, GDPR mandates that any device collecting biometric signals or generating health predictions must comply with strict data processing rules, implement privacy by design and by default (Article 25), and conduct data protection impact assessments for high-risk processing such as advanced health monitoring and systematic location tracking.[20]

The EU AI Act, entering into force in August 2024, introduces the world's first comprehensive AI law, establishing a risk-based classification system that explicitly labels "AI systems intended for medical use" as high-risk.[18,19] Medical device AI systems classified under MDR class IIa, IIb, and III require third-party conformity assessment by a notified body, with compliance obligations for data quality, data governance, record-keeping, transparency, accountability, and human oversight

that extend beyond existing medical device regulations.[18] Full compliance for high-risk systems, including many wearable AI applications, will be phased in through August 2027.[13] Nevertheless, implementation challenges persist, including the complexity of cross-referencing GDPR and AI Act obligations, resource-intensive conformity assessments for SMEs, and ongoing ambiguity regarding the classification of wellness-oriented wearables under the high-risk category.

United States: HIPAA, FDA, and Regulatory Fragmentation

The United States regulatory landscape for wearable IoHT exhibits significant fragmentation. HIPAA protects health information only when handled by covered entities (healthcare providers, health plans, healthcare clearinghouses), leaving the majority of consumer wearable devices outside its regulatory scope.[13] The FDA regulates devices only when they make medical claims, creating a regulatory gap for wellness-oriented wearables that collect identical biometric data without triggering medical device classification. The Federal Trade Commission (FTC) addresses deceptive data practices but lacks healthcare-specific jurisdiction, while the National Institute of Standards and Technology (NIST) provides voluntary AI risk management frameworks without binding authority.[13,37]

Data protection remains fragmented at the state level: California's Consumer Privacy Act (CCPA), Colorado, and other states have enacted privacy laws with widely varying scope, definitions, and enforcement mechanisms. This patchwork produces rapid technology adoption but persistent uncertainty regarding data ownership, algorithmic accountability, and elderly user rights.[36] The average cost of data breaches in the United States surged to $10.22 million in 2025 — 9% higher than the previous year and significantly above the global average — reflecting the aggressive regulatory and legal landscape.[17]

Asia-Pacific: Diverse and Evolving Approaches

The Asia-Pacific region presents the most heterogeneous regulatory landscape for wearable IoHT governance, ranging from mature frameworks to nascent implementation.[13] Singapore maintains the most advanced framework through its Personal Data Protection Act (PDPA, 2012, amended) with advisory guidelines specific to healthcare and active compliance audits. Japan's Act on the Protection of Personal Information (APPI) provides a flexible, mature framework.[38] Thailand's PDPA B.E. 2562 (2019) classifies health data as "sensitive personal data" requiring explicit consent, with active enforcement demonstrated by the first fine (THB 7 million) issued in 2024.[39] China has adopted comprehensive, increasingly restrictive biometric/AI regulations through the Personal Information Protection Law (PIPL) with mandatory consent and AI content labeling requirements.[36]

Indonesia's Personal Data Protection Law (UU PDP, 2022) classifies health data as sensitive personal data, but implementation remains in its early stages with enforcement mechanisms still developing.[40] Malaysia's PDPA Amendment 2024 introduces a risk-based approach for cross-border transfer.[38] The ASEAN region has made significant progress in enacting personal data protection laws; however, substantial differences persist in scope, sensitive data definitions, and cross-border transfer conditions. IoT-specific regulations remain absent in several Asian countries, with IoT service providers generally subject to general data protection laws without healthcare-specific provisions.[38,39]

Cross-Jurisdictional Comparative Analysis

A structured comparison of these regulatory dimensions is presented in Table 1.

Notable contributions to this field include the SPAU-IoT framework by Saka and Das, which established foundational evaluation criteria for elderly IoT security, and the comprehensive IoMT security scoping review by Svandova and Smutny, which mapped the risk assessment landscape across 2018–2023. The comparative analysis reveals three critical findings. First, regulatory fragmentation creates compliance challenges for global wearable device manufacturers, as devices sold across jurisdictions must navigate fundamentally different consent models, data processing rules, and enforcement regimes.[13] Second, the gap between comprehensive regulations (EU) and fragmented approaches (US, ASEAN) produces uneven protection levels, with elderly users in less-regulated jurisdictions facing significantly higher privacy risks. Third, elderly-specific governance provisions are conspicuously absent across all examined regulatory frameworks, despite the unique vulnerabilities of this population.[13,36]

Table 1 Cross-Jurisdictional Comparative Analysis of Governance Frameworks for AI-Powered Wearable IoHT[13,18–20,36–40]

Dimension	EU (GDPR + AI Act)	US (HIPAA + State Laws)	ASEAN (PDPA Variants)
Scope	All personal data, all entities	Only covered entities (HIPAA)	Varies by country
Consent model	Explicit consent, right to withdraw	Varied; HIPAA consent limited	Explicit (TH, ID); varied elsewhere
AI-specific rules	High-risk classification, transparency mandates	Voluntary NIST framework	Draft regulations (TH); minimal elsewhere
Wearable coverage	Comprehensive via GDPR + AI Act	Fragmented; consumer device gap	Significant gaps; developing
Cross-border transfers	Adequacy decisions, SCCs	No federal framework	CBPR (APEC); varied
Enforcement	Strong (4% global annual turnover)	Varied (HIPAA fines + state)	Emerging (TH first fine 2024)
Elderly-specific provisions	Not specific; via vulnerability provisions	Not specific	Not specific

Ethical Dimensions: Autonomy, Consent, and Dignity

Informed Consent in the Context of AI and Cognitive Decline

Elderly populations confront unique challenges in providing informed consent for AI-driven continuous monitoring. Meaningful informed consent requires comprehension of how AI systems process personal data, generate health predictions, and influence care decisions — a demanding cognitive task even for digitally literate individuals.[30] For older adults experiencing cognitive decline, including dementia and Alzheimer's disease, the complexity multiplies: questions arise regarding who provides consent, how proxy consent is managed, how consent is renewed as cognitive capacity fluctuates, and how the balance between beneficence (protection through monitoring) and autonomy (freedom from surveillance) is maintained.[30,33]

The "always-on" nature of wearable IoHT devices compounds consent challenges. GDPR requires that consent be freely given, specific, informed, and unambiguous with clear affirmative action, yet wearable technology users frequently encounter consent bundled within lengthy terms and conditions, making it difficult to ensure genuine understanding of continuous health monitoring and its implications.[20] Withdrawal of consent poses additional challenges when it may affect core device functions essential for health monitoring.[20]

Algorithmic Bias and Health Equity

AI algorithms that are not designed to accommodate the diversity of elderly populations — spanning different ethnicities, socioeconomic backgrounds, comorbidity profiles, and physiological baselines — risk perpetuating bias and discrimination that lead to inequitable healthcare access.[30] Healthcare professionals bear responsibility for ensuring that AI algorithms are designed and trained to minimize bias, with regular auditing, testing across diverse populations, and transparent reporting of model performance across subgroups.[30,31]

Autonomy, Dignity, and Surveillance

AI systems deployed in long-term elderly care must be designed to uphold autonomy and dignity through transparency, explainability, and fairness.[30] Ethical frameworks for AI-powered wearable IoHT in elderly care should encompass: (1) informed consent mechanisms that are accessible and age-appropriate; (2) transparency in AI system functions and decision-making processes; (3) clear accountability structures delineating responsibilities among device manufacturers, healthcare providers, and caregivers; and (4) robust privacy and security safeguards proportionate to the sensitivity of collected data.[30,31]

Proxy Decision-Making and Caregiver Dynamics

Data governance for elderly individuals requires a multisectoral approach. Effective governance demands collaboration among policymakers, healthcare providers, information technology experts, data privacy specialists, and — most critically —

elderly individuals themselves and their families.[41] Caregiver dynamics introduce additional governance complexity: caregivers may simultaneously function as data guardians, consent proxies, and potential surveillance agents, creating conflicts of interest that current regulatory frameworks inadequately address. Establishing clear boundaries for caregiver data access, implementing graduated permission structures, and ensuring mechanisms for elderly individuals to retain meaningful control over their health data even when cognitive capacity diminishes are essential governance priorities.[41]

Toward an Integrative Governance Framework

Synthesis: Components of the Proposed Framework

Based on the comprehensive analysis of regulatory landscapes, technological risks, and ethical dimensions, a five-layer integrative governance framework for AI-powered wearable IoHT in elderly care is proposed (Figure 2):

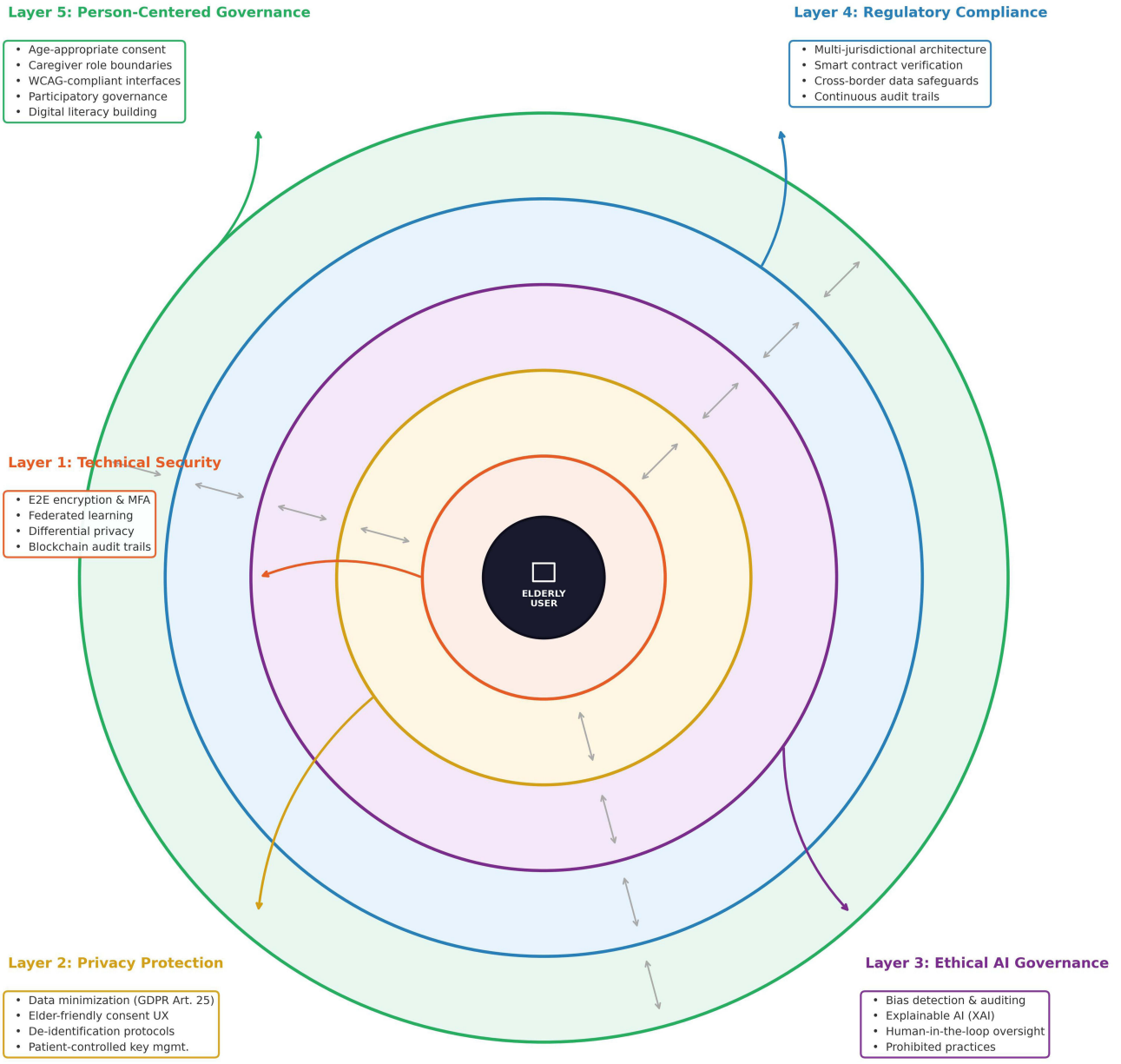

Figure 2 Five-Layer Integrative Governance Framework for AI-Powered Wearable IoHT in Elderly Care. The framework comprises five concentric layers: Layer 1 — Technical Security (encryption, federated learning, blockchain audit trails); Layer 2 — Privacy Protection (data minimization, consent mechanisms, de-identification); Layer 3 — Ethical AI Governance (bias detection, XAI, human-in-the-loop oversight); Layer 4 — Regulatory Compliance (multi-jurisdictional architecture, automated verification); and Layer 5 — Person-Centered Governance (age-appropriate consent, caregiver role boundaries, participatory structures). Arrows indicate bidirectional interactions between layers.

https://doi.org/10.2147/RMHP.S606165

Layer 1 — Technical Security

End-to-end encryption and secure authentication incorporating multi-factor and biometric-friendly mechanisms; privacy-preserving analytics through federated learning and differential privacy; secure-by-default settings with guardianship features enabling progressive access control; and blockchain-based audit trails for immutable transaction records and automated compliance verification.[42,43]

Layer 2 — Privacy Protection

Data minimization principles aligned with GDPR Article 25 requirements for privacy by design; explicit consent mechanisms designed with elderly-friendly interfaces including simplified language, visual cues, audio explanations, and progressive disclosure; privacy-preserving analytics and robust de-identification protocols; and patient-controlled cryptographic key management enabling meaningful exercise of the right to erasure.[20,44]

Layer 3 — Ethical AI Governance

Mandatory algorithmic bias detection and mitigation through regular independent auditing; explainable AI (XAI) requirements for clinical decisions affecting elderly care; human-in-the-loop oversight for high-stakes decisions including medication adjustments, risk stratification changes, and care escalation recommendations; and prohibition of emotion recognition and social scoring applications in elderly care settings, consistent with EU AI Act prohibited practices.[30,31,45]

Layer 4 — Regulatory Compliance

Multi-jurisdictional compliance architecture accommodating GDPR, HIPAA, and PDPA variant requirements; automated compliance verification through smart contracts and continuous monitoring systems; interoperable standards enabling cross-border data transfers with appropriate safeguards; and continuous audit trails maintained through distributed ledger technology.[13,44]

Layer 5 — Person-Centered Governance

Age-appropriate consent mechanisms with dynamic adaptation to cognitive capacity; caregiver role boundaries with clear delineation of access privileges and proxy decision-making protocols; accessible interfaces compliant with Web Content Accessibility Guidelines (WCAG) standards and designed for users with visual, auditory, motor, and cognitive impairments; progressive learning interfaces that build digital literacy gradually; and participatory governance structures ensuring elderly representation in data governance committees.[22,41]

Health Economics Implications

The economic rationale for comprehensive governance frameworks is compelling. With healthcare data breach costs averaging $7.42 million per incident in 2025 and the number of providers reporting losses exceeding $200,000 quadrupling, the cost of governance failure substantially exceeds investment in proactive compliance.[14,15] Privacy-preserving technologies such as federated learning can reduce data centralization costs while maintaining regulatory compliance, and blockchain-based systems can automate compliance verification, reducing ongoing audit expenses.[42,44] Results-based financing models that incentivize privacy preservation and governance adherence could further align economic incentives with ethical imperatives.

Actionable Recommendations

For Governments and Regulators

Adopt risk-based AI classification for health wearables consistent with the EU AI Act model; introduce elderly-specific provisions within existing data protection laws, addressing cognitive decline, proxy consent, and accessibility requirements; harmonize regional regulations, particularly within ASEAN, through health data codes of conduct and mutual recognition frameworks; and mandate regular algorithmic impact assessments for AI systems deployed in elderly care settings.

For Industry and Device Manufacturers

Implement privacy-by-design throughout the product development lifecycle; conduct mandatory bias auditing with elderly-representative validation datasets; design user interfaces specifically for elderly populations through iterative co-design with older adults; and adopt federated learning architectures that maintain data locality while enabling collaborative model improvement.

For Healthcare Providers

Establish data governance committees with multisectoral representation including elderly advocates; implement clear informed consent protocols adapted for varying cognitive capacity; provide training for clinical staff on AI governance, privacy obligations, and ethical monitoring practices; and develop dual-track protocols ensuring continuity of essential care services alongside digital monitoring.

For Researchers

Develop standardized evaluation metrics for governance framework effectiveness; conduct longitudinal studies examining the impact of governance interventions on health outcomes and user trust; build diverse, elderly-representative training datasets for AI model development; and investigate real-world testing of integrative governance frameworks across cultural and regulatory contexts.

Discussion

Contributions and Novelty

This review provides the first integrative analysis that simultaneously examines privacy, security, and governance dimensions of AI-powered wearable IoHT with a specific focus on elderly care within a risk management framework. Unlike prior work that concentrated on technical security frameworks for IoMT generally,[21] or evaluated technical security criteria without governance and policy dimensions,[22] this review synthesizes evidence across technological, regulatory, ethical, and clinical domains to propose a unified governance framework. The five-layer framework advances beyond existing models by explicitly incorporating person-centered governance elements designed for elderly users — a dimension absent from all regulatory frameworks examined.

Alignment with Risk Management and Healthcare Policy

The findings hold direct relevance for healthcare risk management. Privacy and security governance of AI-driven wearable devices constitutes a fundamental risk management challenge affecting patient safety, institutional liability, and healthcare service delivery. The documented regulatory fragmentation — particularly the gap between the EU's comprehensive approach and the US's sector-specific patchwork — creates risk exposure for healthcare organizations operating across jurisdictions. The proposed integrative framework provides a structured approach to risk identification, assessment, and mitigation that aligns with established risk management principles while addressing the unique characteristics of AI-powered wearable technologies and elderly user vulnerabilities.

Limitations

Several limitations should be acknowledged. First, the review was restricted to English-language publications, potentially excluding relevant regulatory analyses and governance frameworks from non-English-speaking jurisdictions. Second, the rapid evolution of both AI technology and regulatory landscapes means that some findings may become outdated as new legislation is enacted and technologies advance. Third, the heterogeneity of governance frameworks across jurisdictions complicates direct comparison, as regulatory philosophies, enforcement cultures, and healthcare system structures differ fundamentally. Fourth, the proposed integrative framework, while theoretically grounded, requires empirical validation through real-world implementation studies. Fifth, the focus on wearable devices may not fully capture governance challenges associated with non-wearable IoHT technologies such as ambient sensors and smart home systems that also serve elderly care functions.

Future Research Directions

Priority areas for future investigation include: (1) empirical testing of the proposed integrative governance framework in diverse regulatory and cultural contexts; (2) longitudinal studies assessing the impact of privacy governance interventions on elderly health outcomes, technology adoption, and user trust; (3) development of AI-specific regulatory provisions for elderly care within ASEAN jurisdictions, where governance gaps are most pronounced; (4) investigation of novel privacy-preserving technologies — including adaptive differential privacy mechanisms that dynamically adjust

protection levels based on data sensitivity and device capabilities[46] — for deployment in resource-constrained elderly care settings; and (5) co-design studies involving elderly users, caregivers, and healthcare professionals to develop governance mechanisms that are both protective and practically implementable.

Conclusion

AI-powered wearable IoHT devices hold transformative potential for improving elderly healthcare through continuous monitoring, early risk detection, and personalized interventions. However, the massive collection of sensitive biometric data, combined with AI-driven analytical capabilities that can infer health conditions beyond the scope of original consent, creates privacy, security, and governance challenges that current regulatory frameworks inadequately address. This comprehensive review of 333 studies reveals three critical findings: first, significant regulatory fragmentation across jurisdictions creates uneven protection and compliance challenges; second, elderly-specific governance provisions remain absent across all major regulatory regimes despite the unique vulnerabilities of this population; and third, existing technical security frameworks insufficiently integrate ethical, regulatory, and person-centered governance dimensions.

The proposed five-layer integrative governance framework — spanning technical security, privacy protection, ethical AI governance, regulatory compliance, and person-centered governance — offers a structured pathway for addressing these gaps. Realizing this framework's potential demands coordinated action: governments must develop elderly-sensitive regulatory provisions, industry must embed privacy-by-design and bias mitigation into product development, healthcare providers must establish robust data governance protocols, and researchers must generate the evidence base for policy refinement. The convergence of rapid technological advancement, an aging global population, and evolving regulatory landscapes creates both urgency and opportunity. A failure to establish adequate governance will erode trust, exacerbate health inequities, and undermine the promise of AI-powered wearable technologies for elderly care. Proactive, evidence-based governance can ensure these technologies enhance the dignity, autonomy, and health outcomes of the world's growing elderly population.

Acknowledgments

We thank the librarians at Universitas Padjadjaran for their support.

Funding

This publication charge is funded by Unpad through the Indonesian Endowment Fund for Education (LPDP) on behalf of the Indonesian Ministry of Higher Education, Science and Technology and managed under the EQUITY Program (Contract No. 4303/B3/DT.03.08/2025 and 3927/UN6.RKT/HK.07.00/2025). The funder had no role in study design, data collection and analysis, decision to publish, or manuscript preparation.

Disclosure

The authors declare that they have no conflicts of interest related to this manuscript.

References

1. World Health Organization. Ageing and health. WHO fact sheet. 2024. Available from: https://www.who.int/news-room/fact-sheets/detail/ageing-and-health. Accessed February, 2026.
2. World Health Organization. Population ageing. 2025. Available from: https://www.who.int/news-room/questions-and-answers/item/population-ageing. Accessed February, 2026.
3. United Nations, Department of Economic and Social Affairs. World population ageing 2024. New York: United Nations; 2024.
4. Eurostat. Population structure and ageing. Statistics Explained. 2025. Available from: https://ec.europa.eu/eurostat/statistics-explained/index.php/Population_structure_and_ageing. Accessed April 16, 2026.
5. Grand View Research. Internet of medical things (IoMT) market size, share & trends analysis report. 2025. Available from: https://www.grandviewresearch.com/industry-analysis/internet-of-medical-things-iomt-market. Accessed April 16, 2026.
6. Mordor Intelligence. Internet of medical things market size & share analysis – growth trends & forecasts (2024–2030). 2025. Available from: https://www.mordorintelligence.com/industry-reports/internet-of-medical-things-market. Accessed April 16, 2026.
7. Grand View Research. IoT wearable device market size & trends analysis report, 2024–2030. 2024. Available from: https://www.grandviewresearch.com/industry-analysis/iot-wearable-device-market-report. Accessed April 16, 2026.
8. Huang GQ, Chen XF, Liao CZ. AI-driven wearable bioelectronics in digital healthcare. *Biosensors*. 2025;15(7):410. doi:10.3390/bios15070410

9. Qian Y, Siau KL. Advances in IoT, AI, and sensor-based technologies for disease treatment, health promotion, successful ageing, and ageing well. *Sensors*. 2025;25(19):6207. doi:10.3390/s25196207
10. Tang C, Zhang R, Gao S, et al. An AI-driven multimodal smart home platform for continuous monitoring and assistance in post-stroke motor impairment. *IEEE Trans Neural Syst Rehabil Eng*. 2026;34:1–14. doi:10.1109/TNSRE.2025.3645093
11. Naseer F, Addas A, Tahir M, Khan MN, Sattar N. Integrating generative adversarial networks with IoT for adaptive AI-powered personalized elderly care in smart homes. *Front Artif Intell*. 2025;8:1520592. doi:10.3389/frai.2025.1520592
12. Ghosh S, Ghosh SK. FEEL: federated learning framework for elderly healthcare using edge-IoMT. *IEEE Trans Comput Soc Syst*. 2023;10 (4):1841–1853. doi:10.1109/TCSS.2022.3233300
13. Khan F, Touritz P, Hua D. AI-powered privacy-preserving models and IoT solutions for elderly healthcare: a comprehensive survey. In: *Proceedings of the Information Systems Education Conference (ISECON)*. Portland, OR: EDSIG; 2024.
14. IBM Security. Cost of a data breach report 2025. 2025. Available from: https://www.ibm.com/reports/data-breach. Accessed February 2026.
15. US Department of Health and Human Services. Healthcare data breaches: annual report 2025. Washington, DC: HHS Office for Civil Rights; 2025.
16. HIPAA Journal. Healthcare data breach statistics 2025. 2025. Available from: https://www.hipaajournal.com/healthcare-data-breach-statistics/. Accessed February 2026.
17. Ponemon Institute. Cost of healthcare data breaches in the United States: 2025 report. 2025.
18. European Parliament and Council. Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (AI Act). *Off J Eur Union*. 2024;L 2024/1689:1–144.
19. Reed Smith LLP. The EU AI Act and medical devices: navigating high-risk compliance. 2025.
20. European Parliament and Council. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (GDPR). *Off J Eur Union*. 2016;L119:1–88.
21. Svandova K, Smutny Z. Internet of medical things security frameworks for risk assessment and management: a scoping review. *J Multidiscip Healthc*. 2024;17:5075–5094. doi:10.2147/JMDH.S484509
22. Saka AO, Das D. SoK: reviewing two decades of security, privacy, accessibility, and usability studies on Internet of Things for older adult. *arXiv preprint*. 2025;arXiv:2512.16394. doi:10.48550/arXiv.2512.16394
23. Tricco AC, Lillie E, Zarin W, et al. PRISMA extension for scoping reviews (PRISMA-ScR): checklist and explanation. *Ann Intern Med*. 2018;169 (7):467–473. doi:10.7326/M18-0850
24. Posada-Quintero HF, Chon KH. Innovations in electrodermal activity data collection and signal processing: a systematic review. *Sensors*. 2020;20 (2):479. doi:10.3390/s20020479
25. Sykes ER. Next-generation fall detection: harnessing human pose estimation and transformer technology. *Health Syst*. 2025;14(1):1–21. doi:10.1080/20476965.2024.2395574
26. Tan JF, Suratman FY. Real-time fall detection with hybrid CNN-LSTM using IWR6843AOP FMCW radar. *IEEE Access*. 2025;13:1–15. doi:10.1109/ACCESS.2025.3605387
27. Salvi S, Garg L, Gurupur V. Stage-wise IoT solutions for Alzheimer's disease: a systematic review of detection, monitoring, and assistive technologies. *Sensors*. 2025;25(17):5252. doi:10.3390/s25175252
28. Azizatunnisa R, Ghozali MT. Improving medication adherence in elderly patients through IoMT-enabled smart pill dispensers: a narrative review. In: *Proceedings of the 5th International Conference on Emerging Smart Technologies and Applications (eSmarTA)*. IEEE; 2025. doi:10.1109/eSmarTA66764.2025.11132209.
29. Diniz P, Grimm B, Garcia F, et al. Digital twin systems for musculoskeletal applications: a current concepts review. *Knee Surg Sports Traumatol Arthrosc*. 2025;33(1):1–16. doi:10.1002/ksa.12627
30. Jain V, Mitra A, Haque A. Integrating AI in assistive devices for cognitive support in the elderly: design, usability, and ethical frameworks. In: AI-Augmented HCI: Advances, Challenges, and Applications. IGI Global; 2025:589–622. doi:10.4018/979-8-3693-8034-5.ch027.
31. Radanliev P. Privacy, ethics, transparency, and accountability in AI systems for wearable devices. *Front Digit Health*. 2025;7:1431246. doi:10.3389/fdgth.2025.1431246
32. Dutta J, Puthal D. Advancing eHealth in Society 5.0: a fuzzy logic and blockchain-enhanced framework for integrating IoMT, edge, and cloud with AI. *IEEE Access*. 2024;12:192405–192423. doi:10.1109/ACCESS.2024.3520799
33. Hasan MM, Anik FI, Rodriguez-Cardenas J, et al. IoMT and data privacy in Alzheimer's care for older adults: a systematic review. *EAI Endorsed Trans Pervasive Health Technol*. 2025;11:e6170. doi:10.4108/eetpht.11.6170
34. Zhou A, Piramuthu S. Smart IoMT applications in senior healthcare: balancing functionality, security, and privacy challenges. In: *Proceedings of the IEEE International Conference on Mobile Security and Privacy (MobiSecServ)*. IEEE; 2024:1–6. doi:10.1109/MobiSecServ63327.2024.10760186.
35. Grigorovich A, Harvey K, Levy A, et al. Real-time location system implementation in dementia care: stakeholder perspectives. *Gerontologist*. 2025;65(3):gnaf244. doi:10.1093/geront/gnaf244
36. Ksibi S, Jaidi F, Bouhoula A. A comprehensive study of security and cyber-security risk management within e-health systems: synthesis, analysis and a novel quantified approach. *Mob Netw Appl*. 2022;27(6):2313–2328. doi:10.1007/s11036-022-02042-1
37. Devaraj P, Deepalakshmi P. Improvement of Internet of Health Things (IoHT) devices: cybersecurity challenges on unauthorized access and privacy breach in healthcare settings. In: 2025 IEEE World Conference on Applied Intelligence and Computing (WCONF). IEEE; 2025. doi:10.1109/WCONF64849.2025.11233430.
38. Chen Y, Liu L, Wu Q, Yang CF. Proactive and adaptive elderly-centered governance framework through synergistic integration of the internet of things and multi-agent systems. *Sens Mater*. 2025;37(2):555–575. doi:10.18494/SAM5741
39. Aleksandrova K. The right to erasure and its implication on AAL systems. In: International Multidisciplinary Conference on Innovative Scientific Approaches. 2021:1–12.
40. Islam U, Ullah H, Khan N, Ahmad I, Saleem K. Adaptive federated learning framework for privacy-preserving consumer-centric IoMT: a novel secure data collaboration model. *IEEE Trans Consum Electron*. 2025;71(3):1–14. doi:10.1109/TCE.2025.3606642
41. Cejudo A, Tellechea Y, Calvo A, et al. Scalable big data platform with end-to-end traceability for health data monitoring in older adults: development and performance evaluation. *JMIR Aging*. 2025;8:e81701. doi:10.2196/81701
42. Khan H, Kavati R, Pulkaram SS, Jalooli A. End-to-end privacy-aware federated learning for wearable health devices via encrypted aggregation in programmable networks. *Sensors*. 2025;25(22):7023. doi:10.3390/s25227023

43. Alsenani Y. FAItH: federated analytics and integrated differential privacy with clustering for healthcare monitoring. *Sci Rep*. 2025;15(1):10155. doi:10.1038/s41598-025-94501-4
44. Mohammed AS. Homomorphic encryption with blockchain for securing data in healthcare industry-based IoT. *Hum Centric Comput Inf Sci*. 2024;14:016. doi:10.22967/HCIS.2024.14.016
45. Ali A, Montanaro T, Sergi I, et al. An innovative IoT and edge intelligence framework for monitoring elderly people using anomaly detection on data from non-wearable sensors. *Sensors*. 2025;25(6):1735. doi:10.3390/s25061735
46. Mazid A, Kirmani S, Abid M, Pawar V. A secure and efficient framework for internet of medical things through blockchain driven customized federated learning. *Cluster Comput*. 2025;28(3):1–18. doi:10.1007/s10586-024-04896-4