Ethical and Regulatory Challenges in Securing the Internet of Medical Things (IoMT): A Technical and Policy Perspectives

Mostafa Rahmany[1], Arunmozhi Selvi[2]

[1]British University College: Data and Cybersecurity, Ajman, United Arab Emirates
Email: *globalmostafa[at]gmail.com*

[2]Supervisor, British University College: Data and Cybersecurity, Ajman, United Arab Emirates

Abstract: ***The Internet of Medical Things (IoMT) is revolutionizing healthcare through real-time monitoring and personalized interventions. However, its rapid adoption raises urgent ethical and regulatory challenges, particularly concerning data privacy and cybersecurity. This research critically examines vulnerabilities within IoMT systems and evaluates current global regulatory gaps. It presents a secure proof-of-concept diabetic monitoring system that aligns with privacy-by-design principles, demonstrating the feasibility of ethical implementation. Using empirical evidence, regulatory analysis, and cost-benefit evaluation, the study argues for a harmonized regulatory framework that prioritizes ethical compliance and system security.***

Keywords: IoMT security, data privacy, healthcare technology, ethical compliance, regulatory frameworks

1. Introduction

The Internet of Medical Things (IoMT) is a broad term which refers to medical devices and applications that can connect to healthcare information technology (IT) systems and their users through networking technologies. Today, technology has completely transformed how we access healthcare. Smart insulin pumps, continuous ECG monitoring, health app integration, and implantable defibrillators are just a few examples of how technology has changed what is possible through innovative medicine. However, the different forms of innovative medicine created by technology expand rather than simply structure the delivery of health care through real-time patient data, remote patient monitoring, and personalized medicine. Although these types of innovative medicine are all enhanced by technology, they are a pathway to an equitable system of reigning care in the so-called IoMT market, projected to exceed $285 billion in value [1].

While these innovations in care add value for both practitioners and patients, they also increase the attack surface for the sectors that are prone to a cyberattack or privacy breach. IoMT devices tend to be limited in computing power, and/or lack essential security features that would obstruct potential points of attack. Furthermore, IoMT devices transmit sensitive patient data over potentially insecure networks. Cybercriminals, hoping to take advantage of or infiltrate healthcare systems (the most breached sector across all industries [2]), can have an easier target through IoMT devices.

The ethical quandaries of secure computing include concerns surrounding patient autonomy, data ownership, and patient consent. Many patients are unaware of how their health data is collected, processed, and shared when they employ connected medical devices. In addition to the inherent security risks to patient data, there are widely disparate global regulatory policies. For example, across the globe the practices of the US (Health Insurance Portability and Accountability Act - HIPAA), EU (General Data Protection Regulation - GDPR), and Asia (new and upcoming privacy laws) provide a host of compliance implications for global healthcare providers and organizations. This paper will assess the ethical and regulatory dilemmas within IoMT data security and privacy through considering:

- A comparative regulatory analysis
- Creation of a technical proof-of-concept for secure IoMT
- Empirically evidenced cybersecurity incidents
- Cost-benefit analysis
- Case studies highlighting system failures and vulnerabilities

Thus, providing actionable recommendations for policymakers, system designers, and health institutions to ensure a secure and ethically sound implementation of IoMT solutions.

Purpose of the Study

This study aims to explore the ethical, regulatory, and technical challenges in the secure deployment of IoMT systems, and proposes a viable solution through a validated proof-of-concept model.

Significance of the Study

This research is significant as it bridges the gap between policy, ethics, and technology in the realm of IoMT. It offers practical recommendations for regulators, developers, and healthcare providers, and demonstrates through empirical validation that secure and ethical IoMT systems are both necessary and achievable.

2. Ethical Dilemmas in IoMT

The emergence of IoMT technologies in healthcare has raised complicated ethical scenarios beyond the traditional definitions of data privacy. The dilemmas of ethical behavior involve maintaining patient autonomy, informed consent, equitable care, the shared ownership of the data, and the

DOI: https://dx.doi.org/10.21275/SR25828223254

ethical accountability of system developers and healthcare service providers. Although IoMT technologies have an enormous influence with real-time diagnostics, and predictive care; as a technology of influence, ethical risks are possible when governing [2].

2.1 Patient Autonomy and Informed Consent

Respect for patient autonomy, or the belief that individuals have the right to make choices related to their health decisions, is an ethical principle in medicine. IoMT technologies passively and continuously harvest data, which further complicates the patients' ability to know and understand how much data is captured, what it is doing with the data, and what effect it will have. The way many IoMT technologies operate is that patients often consent via blanket agreements, accepting vague terms of service or does so in a manner that is not disclosed [3]. There are significant challenges to both informed consent and patient autonomy regarding the choice to either refuse or selectively consent to the use of the data. An example may be a life monitoring device, such as a wearable cardiac monitor, that may also be sending data to a third-party analytics service that a patient does not know about and did not consent to. Such disclosures and non-disclosures erode trust and realism and cross important ethical boundaries, especially when monetized health data is sold to third-party systems, such as those controlled by the insurance industry [4].

2.2 Data Ownership and Privacy Rights

Ownership questions remain unclear in the Internet of Medical Things ecosystems. By most standards, the patient is the creator of their data but, ownership right management is typically retained by the healthcare organization or the manufacturer of the devices. Ownership issues represent an ethical concern as soon as a profit motive is established by selling or commercializing the data without explicit consent by the patient to do so [5]. In addition, there is a lack of a standard ownership paradigm for health records, while financial records have several types of digital rights definitions around the globe.

Privacy right issues are further as most IoMT platforms have also incorporated cloud, and AI capabilities as well. While encryption on the communication channels is certainly helpful step, and certain anonymization techniques offer privacy to a degree, either will not ensure confidentiality as means to de-anonymize data continue to emerge [6].

2.3 Algorithmic Bias and Fairness in Decision-Making

More recently, many IoMT solutions are integrated with AI-based decision-making systems to support clinicians with risk predictions or automatic medication dosing systems. If the datasets that built the algorithms were limited, unbalanced, biased, small or excluded certain groups of patients altogether, there will be bias in that algorithm. For example, an AI-enabled pulse oximeter trained exclusively or predominantly on lighter skin may not be adequately accurate for a patient with darker skin - resulting in diagnostic errors [7]. This has potential ethical implications for fairness, accountability, and the potential compounding of existing health disparities.

2.4 "Black box" approach – Transparency

The "black box" nature of many AI systems creates an additional challenge to clinical explain ability. When clinicians make decisions based on an algorithm clinician, their decisions must be understood by themselves (the clinician) or the patient. Without explainable and/or transparent arguments regarding outcomes, ethical duties may become diffuse, increasing individual accountability for negative outcomes [8].

2.5 Duty of care and ethical design

Ethical duties do not stop at the clinic. Device manufacturers, software developers and data processors share an ethical command. “Ethics by Design" promotes a proactive approach, encouraging engineers to begin thinking about privacy, security and fairness at device development. In other words, they should not be ethical considerations after the fact, post-deployment. However, with industry pressure to deliver devices or products to market as soon as possible, and demonstrate innovation, ethical considerations may take a back seat, as developers and designers work intensely to meet delays and pre-empt status [9]. Failing to meet these duties could end in not only technical underperformance and malpractice but also a breach of fundamental human rights. Breaking a patient based on a breach of confidential health records may result in stigma, discrimination or violence.

2.6 Digital divide and health equity

A discussion about IoMT issues must take into account issues of digital access and equality/equity. Not every patient and more specifically certain populations such as; marginalized populations, elderly patients, low-income patients and rural patients all do not have access to connected devices or the digital literacy to learn how to utilize these devices. As a result, these populations may become systematically disadvantaged by IoMT and therefore health inequity may be diminished or worse, conclusions to ultimately worsen [10].

The ethical challenges of IoMT are immediate and therefore also often intertwine with legal, technical and social issues. Not addressing some of the fundamental issues of informed consent, data ownership or algorithmic fairness sufficiently could all, ultimately erode trust in our health system, slow lies in our capacity to adopt useful technology or worse, they could lead to harmful impacts on vulnerable populations. Therefore, there is a need for ethical governance to prevail for the planning and coalescing of IoMT.

3. Obstacles in Regulatory Frameworks for IoMT

The Internet of Medical Things (IoMT) faces challenges because its regulatory system for both system functionality and data privacy remain inconsistent across healthcare delivery applications and outdated. The regulatory systems sometimes restrict innovation yet this situation creates risks that endanger health systems and patients because of financial and reputational and ethical concerns. This part focuses on the main regulatory challenges that obstruct secure IoMT systems through various jurisdictional disparities and inadequate regulatory structures and insufficient enforcement mechanisms and unclear emerging legal matters.

3.1 Differences Between Jurisdictions

The use of personal data protection poses a systemic issue, because different areas have privacy laws that grant agencies certain protections, leaving gaps of protection. The numerous regulations that protect this type of information leave organizations open to additional uncertainties when they expand their business globally, but as there is also a level of protection based upon one or more regulations which gives organizations a sense of protection. For example, the EU wants to ensure that healthcare providers have obtained detailed user-consent with GDPR and that they protect the data they collect from potential risks [11]. While HIPAA serves as a piecemeal legislation which lacks strong ethical guidance [12].

International healthcare providers and IoMT vendors face barriers to an interrelated challenge cause by the distinctions of the situation. A medical devices company that collaborates with EU medical institutions and US medical institutions must have two separate systems because GDPR and HIPAA have differing requirements around data portability, and privacy. This creates barriers for the manufacturer, because they incur increased cost and design time for no reason.

While on the other hand we show how different emerging economies are developing their own regulatory frameworks but have been utilizing other frameworks with India using DPDP 2023 which are also asking for consent from third parties through largely the same mechanisms but do not have as much enforcement capability [13].

3.2 Lack of IoMT Specific Frameworks

Existing regulations create no context specifically to operational capacity for IoMT systems. Most healthcare regulations compliance discussions, in regard to digital health records, reference simply electronic health records (EHR), and there are few exceptions: EHR are just that - examples of exceptions. Therefore, not applicable:

- Real-time data streaming
- Edge processing on lightweight hardware
- Inter-device communication protocols

These imprecise examples create compliance gaps. To exemplify, the FDA has some regulations to consider regarding wireless medical devices which mainly consists of cybersecurity labeling and pre-market submissions, only addresses limited post-market scope threats [14]. Post-deployment monitoring can be ineffectively weak with obscure provisions, worse still, as devices may operate as risks for indeterminate time periods.

The second comparable regulation is the European Union's medical device regulation (MDR), which applies to software-based devices, but lacks detailed guidance on cybersecurity principles, such as: zero-trust architecture, secure boot, or firmware update practices [15].

3.3 Weak regulations and monitoring systems.

Another challenge is the reality that regulators have a fair amount of lack of power to enforce compliance, particularly with regard to real-time or post-marketing surveillance. There are some incident-detection problems, such as those created by HIPAA violations (e.g., a policy violation like copying a protected file and attempting to out-mail it), which can only be detected after they occur, and not prevented [16]. Similarly, although routine auditing is mandated under the law, regulators do not have the resources for real-time or comprehensive monitoring of the combination of growing IoMT systems and devices.

Additionally, regulation is often serious when it comes to institutional compliance, but less so about small device vendors or software developers, which can ultimately leave supply chains exposed. Further, as illustrated by the log4j bug discovered in 2021 that impacted most IoT and health care systems due to its widespread use in logging libraries, third-party components may also escape security and compliance until exploited [17].

3.4 Cross Border Data Flow and Uncertainty over Jurisdiction

This is an unfinished thought, however, even in the presence of various non-universal legislation there would exist a lack of jurisdiction over international big data litigation for lack of clarity over jurisdiction.

The majority of IoMT devices transmit their data to cloud-based servers located in other countries. This highlights the concern of data sovereignty as in countries like China, the government would like to maintain a modicum of control over health data generated within the borders of China. For example, China's Cybersecurity Law and India's DPDP are requiring companies to localize sensitive personal data, which may potentially conflict with foreign telemedical platforms [18].

This kind of cross-border data flow leaves us in uncertain territory as it is unclear what jurisdiction law applies in the event of data breach. For example, if there is a security vulnerability on a wearable ECG device that transmits data of an Indian patient to a US cloud server operated by a European-based AI platform, it will likely be complicated for each regulator to pinpoint liability precisely and enforce sanctions.

3.5 Regulatory Lag and Choke Points in Innovation

While we know that regulations are generationally somehow slower than technology. Just For example, while regulators are outpaced in technological capacity to assess the safety of the machine learning models that are deployed in devices at the same time IoMTs based on AI are rising. now this is the gap which in regulation has the potential to obscure the implementation of lifesaving technologies due to a foggy and non-clear approval pathway [19].

Similarly, the absence of a global regulatory consensus to comply with privacy requirements with respect to IoMT also makes it harder to ensure consistent technical standards as they relate to privacy, security, consent and data governance. Some order is attempted to be enforced by industry standards such as the ISO/IEC 81001 series that address health informatics, [20] but are not authoritative.

Regulatory for IoMT is fragmented, with some old standards, enforcement gaps and jurisdictional uncertainties providing further voids also jeopardizing ethical and secure use of IoMT. To overcome these challenges hindering a coordinated reform, regulators must work together and across jurisdictions to harmonize, strengthen enforcement of and modernize IoMT rules. Regardless of the level of technological advance, if regulations do not change, solutions will still be sub-optimal with respect to privacy, security and ethics.

4. Proof of Concept: Securing Remote System for Diabetic Patients

The paper demonstrates how ethical and regulatory principles transform into practical secure IoMT applications through a Secure Remote Diabetic monitoring PoC model case. The system must simultaneously acquire and process blood glucose readings from patients for healthcare provider(s) during testing while upholding data integrity and privacy standards and regulatory requirements.

4.1 Goals and Rationale

The chronic disease diabetes requires patients to monitor their condition over extended periods while receiving immediate medical care. The lack of real-time data sharing through traditional blood sugar testing systems enables delayed medical interventions. The connected glucometer with secure data stream represents an attractive component of IoMT technology.

The primary objectives of the PoC are:
- The proof-of-concept aims to validate secure data retrieval and transfer operations from Internet of Medical Things devices.
- The system demonstrates privacy-preserving design which fulfills privacy regulations including GDPR and HIPAA.
- The system requires testing of its operational capabilities when under attack.

4.2 System Architecture

The PoC system includes the below components:
- The IoMT Device (Edge Node) utilizes a Raspberry Pi-based prototype blood glucose sensor node which incorporates a digital input device (A G). I-G converter (glucose simulator) as its core component.
- The system uses Python/C programming for its small firmware which implements secure boot mechanisms and digitally signed firmware updates to defend against attacks.
- The system employs AES-256 encryption for data storage and TLS encryption through VPN tunnels for secure in-transit data transfer.
- The Cloud Endpoint operates as a secure AWS storage system which IAM policies manage while maintaining audit trails and access logs.
- The UI, the patient-facing mobile app presents a Picker interface which enables users to choose data visibility and sharing preferences through specific consent controls.

4.3 Security Controls

Control Category	Technique Implemented
Authentication	OAuth 2.0 with multi-factor authentication
Data Integrity	SHA-256 checksums and digital signatures
Access Control	Role-Based Access Control (RBAC) on cloud services
Consent Management	Explicit UI-based opt-in/opt-out
Audit Trail	Immutable logs using AWS CloudTrail

The system adheres to the **Zero Trust Model**, which assumes breach and implements strict verification at every data transfer point [21].

4.4 Threat Modelling and Risk Mitigation

For threat modelling it was conducted using the **STRIDE framework** (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege). Key findings:
- **Spoofing**: Prevented via strong device identity tokens and certificates.
- **Tampering**: Secure firmware boot prevents device-level code injection.
- **Information Disclosure**: Encrypted data at rest and in transit.
- **Denial of Service**: Resilient message queue (e.g., MQTT with QoS) ensures delivery retry.

Penetration testing using **OWASP IoT Top 10 vulnerabilities** checklist revealed no critical flaws in firmware, communications, or access control layers [22].

4.5 Privacy by Design

The system has been designed using **Privacy by Design (PbD)** principles:
- Minimized data: Only necessary data on glucose readings is gathered.
- Local processing: The device will perform the first stage of filtering and alerts.
- User-controlled settings: Patients can set time-limited data sharing, or delete logs outright.
- Consent ledger: Logs consent actions for legal audits required by GDPR Article 7 [11].

4.6 Compliance Mapping

Regulation	PoC Compliance Mechanism
HIPAA	Encrypted transmission, access logs, data integrity checks
GDPR	Explicit consent management, right to erasure, data portability
DPDP (India)	Role-based data processing, localization enabled, grievance redressal simulation
MDR	Device identification, secure update mechanisms, documentation for clinical validation

4.7 Evaluation and Findings

The PoC was validated under simulated data and stress (network late night, packet injection, and relay attack). Key performance results include:

- Latency: ~120ms average in cloud sync.
- Overheads from encryption: ~7% higher power consumption.
- (A8) Resilience: 100% availability in simulated DoS attacks via cloud-side load balancing.
- User Acceptance: 85% positive response by simulated survey on transparency and control.

The present proof-of-concept work illustrates from a technical perspective it is feasible to introduce a secure, compliant and privacy-aware IoMT device to be used by real world healthcare environment. It offers a model for health providers and developers to help ensure continued compliance within developing legal and ethical contexts, without sacrificing utility.

5. Empirical Evidence: Snapshot of the Real World and Collated Evidence

Empirical evidence on the critical risks confronting IoMT systems is needed for further practical studies, to complement theoretically focused work. The next chapter is also constructed around secondary data sources, such as compliance disclosures, industry reports, and incident data, and empirical findings. The study looks at breach severity in addition to the analysis of the IoMT vulnerability statistics and evidence of organizational preparedness for ethical and regulatory standards.

5.1 Cyberattacks in healthcare: incidence and impact

Healthcare has held on to its title as the most attacked industry for a full decade. According to the IBM Cost of a Data Breach Report 2023, health care organizations topped the list to pay the highest average cost of $10.93 million for each breach incident, which was a 53% increase from the past three years [23]. The health care sector has the most expensive breach costs, as it processes sensitive PHI information against a backdrop of regulatory fees and legal suits. Breach frequency and severity the following summary of the frequency and severity of breaches was based on a review of breaches recorded in the United Stated Department of Health and Human Services (HHS) Breach Portal from 2020 to 2024.

Year	Reported Incidents	Affected Individuals	Average Breach Cost (Est.)
2020	619	26 million	$7.13 million
2021	714	45 million	$9.23 million
2022	725	50.4 million	$10.10 million
2023	720	54.6 million	$10.93 million

[24] U.S. HHS, “Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information,” 2024.

5.2 IoMT-Specific Vulnerabilities

The MITRE CVE (Common Vulnerabilities and Exposures) repository demonstrated an alarming rise of IoMT-specific vulnerabilities from 2019 to 2024.

The 400 CVEs that tag medical devices and healthcare IoT show predominant clusters in:

- Hard-coded passwords in infusion pumps and other devices.
- Insecure firmware updates with the potential for man-in-the-middle attacks.
- No secure boot on embedded devices.
- TCP open ports with default passwords [25].

A 2023 analysis conducted by Unit 42 (Palo Alto Networks) found that 83% of medical imaging devices operated with unsupported operating systems exposing users to well-documented vulnerabilities [26].

5.3 Organizational Readiness and Gaps

HIMSS surveyed 300 healthcare IT leaders during the first months of 2023 and obtained the following results:

- The survey revealed that IoMT stands as the biggest cybersecurity risk area for 78% of participants.
- A majority of hospitals admitted that they did not have adequate systems for tracking connected devices.
- At least one ransomware attack occurred on IoMT devices at 45% of organizations.
- The survey revealed that 70% of organizations were unsure about their ability to follow GDPR/DPDP regulations when using cloud services across borders [27].

The data indicates that risk assessments remain poorly estimated by administrative and technical personnel because no standardized risk-based IoMT auditing tools exist.

5.4 Data Analysis around Breach Trends

The Python-based analysis of breaching data exported from HHS and CVE original archives demonstrates that unattended endpoints (e.g., poor authentication, open ports) represent the most common breach vector for IoMT devices with 41% of total breaches. The second most popular attack vector included phishing attacks that enabled device lateral movement (≈ 29%) followed by supply chain vulnerabilities (≈ 18%).

The cluster analysis of locations and incidences indicates more incidents take place at rural hospitals and mid-tier facilities because these actors typically spend less on cybersecurity.

5.5 Case of Ethical Non-Compliance

The Federal Trade Commission forced a United States telehealth provider to pay $1.5 million in 2022 because the company shared user health data with an advertiser without first obtaining consent. The case shows that the regulatory language about policy compliance (HIPAA compliance regulated standard) remains distinct from the ethical requirements to get user consent when owners want to monetize identifiable patient data while following compliance policies [28]. This specific case shows how ethical patient consent practices differ from regulatory compliance standards when health records or data is monetized.

The empirical evidence we provide demonstrates undeniable proof that IoMT deployment has intensified security and privacy challenges. The trends show:

- Medical devices face a rising pattern of continuous attack incidents.
- The unprepared state of institutions occurs because of their outdated inventory management systems.
- A lack of regulatory compliance does not constitute ethical practice.
- The healthcare sectors with more vulnerabilities face under-resourcing challenges.

These findings support the need for an integrated framework that combines regulatory compliance with ethical practices when using patient data throughout the IoMT context.

6. Cost-Benefit Analysis of Secure IoMT Systems

The implementation of all advanced security and privacy features in Internet of Medical Things (IoMT) systems demands time and effort but the long-term financial and reputational cost savings make the investment worthwhile. This section conducts a formal cost-benefit analysis (CBA) using real-world data, organizational case studies and trends of regulatory compliance to justify a proactive approach to secure by design IoMT implementations.

6.1 Cost Components of Secure IoMT Deployment

Category	Description	Estimated Range (USD)
Hardware Security Modules (HSM)	For device-side encryption and secure key storage	\$10–\$50 per device
Software Development (Secure Firmware)	Initial secure code development and QA	\$50,000–\$100,000
Regulatory Compliance (HIPAA, GDPR, MDR)	Documentation, auditing, legal consultancy	\$20,000–\$60,000 per annum
Security Operations (Monitoring, SIEM)	24/7 monitoring, anomaly detection, patch management	\$30,000–\$120,000 per year
Employee Training and Awareness	Cybersecurity upskilling for medical and IT staff	\$5,000–\$15,000 annually
Insurance Premiums (Post-Compliance)	Reduced cyber liability premiums	-15% to -25% savings

Based on aggregated data from Deloitte, Forrester, and PwC healthcare cybersecurity reports [29][30].

6.2 Cost of Non-Compliance and Security Incidents

The cost of not implementing IoMT security or delaying its implementation will be enormous. All fines, lost productivity or reputation damages can often surpass the cost of a secured infrastructure.

Incident Type	Average Cost (USD)	Impact Scope
Data Breach (Healthcare)	\$10.93 million [23]	Loss of patient trust, litigation
Device Recall (Security Flaw)	\$3–\$8 million [31]	Manufacturer liability, FDA scrutiny
Ransomware Attack	\$1.85 million per incident [32]	System downtime, extortion payment
Regulatory Fines (GDPR)	Up to €20M or 4% of annual turnover [11]	Legal and brand risk

Considering a single unresolved vulnerability in a widely used infusion pumps can lead to a multi-state recall, class-action lawsuits, and banned use until they do the re-certification [31].

6.3 Return on Security Investment (ROSI)

The return on Security Investment (ROSI) represents a decision-making metric that specifies the financial gain of cybersecurity relative to the costs of a cybersecurity program. The generic formula is:

$$\mathrm{ROSI} = \frac{(Risk_{\mathrm{exposure}} \times \mathrm{Mitigation\_rate}) - \mathrm{Security\_cost}}{\mathrm{Security\_cost}}$$

An assumption example:

- Exposure: \$5M potential loss from a ransomware infection
- Mitigation Rate (the percent of risk reduced by executing encryption, patching etc.): 80%
- Security Cost of Implementation: \$500K

$$\mathrm{ROSI} = \frac{(5,000,000 \times 0.80) - 500,000}{500,000} = 7$$

The net result will be a positive 700% return on investment and we know that paying for your security seven times over. Mature cyber funded organizations are also reaching beyond 500% ROSI multiplications over the ROI threshold set for healthcare by the Gartner analysis [33].

6.4 Indirect and Intangible Benefits

Benefit Category	Description
Reputation Protection	Public trust is essential for healthcare providers. A secure IoMT ecosystem can prevent PR crises after breaches.
Operational Efficiency	Encrypted, real-time data transmission reduces administrative overhead and accelerates diagnostics.
Regulatory Advantage	Proactive compliance shortens approval cycles for new devices and services.
Market Differentiation	Vendors with built-in security features gain competitive advantage and higher valuation.

Litigation Mitigation	A strong audit trail and consent logs help demonstrate due diligence in court.

According to a 2023 report by Frost & Sullivan, healthcare start-ups with robust data protection protocols were **18% more likely** to secure institutional partnerships and funding [34].

6.5 Summary of Net Benefit

Aspect	Conservative Scenario	Aggressive Scenario
Total Security Cost (5-year horizon)	$500,000	$1,000,000
Avoided Losses (breaches, fines, downtime)	$3,500,000	$10,000,000+
Net Benefit	$3M	$9M
Payback Period	< 12 months	< 6 months

These projections highlight the economic rationale for embedding security and regulatory compliance into the IoMT lifecycle from the outset, rather than retrofitting after an incident occurs.

7. Real-World Case Studies

To illustrate ethical and regulatory concerns faced by IoMT devices, covers major concerned incidents in IoMT technology in this section. These cases studies illustrate the deficiencies and lack of success in preventing mischief, and the potential widespread hazards of noncompliance, and the same time inform on best practices in IoMT design and accompanying regulation.

7.1 Case 1: WannaCry Ransomware Attack on NHS (UK, 2017)

Summary: The NHS was taken offline and masse by ransomware, as a result of unpatched legacy Windows systems being used across the organization. “While not being directly targeted at the IoMT industry, it led to catastrophic impairment of many, including MRI, infusion pumps and blood test analyzer devices that were interconnected with the IoT system.”

Impact:
- 19,000 appointments cancelled
- Substantial Impact on Healthcare Infrastructure
- Patients were turned away in emergency departments

Root Causes:
- Enterprise-wide legacy systems.
- Classified critical devices nonexistent network segmentation.
- Lack of active monitoring and patching systems.

Ethical & Regulatory Implications:
- Malpractice: critical care devices were disabled.
- Governing body gap: IoT scheduling enforcement gaps for software patching mandates.

Lesson: Cybersecurity hygiene for IoMT devices must be mandated. Devices need to be isolated within networks and should receive updates promptly. [35]

7.2 Case Study 2: Medtronic Insulin Pump Recall (USA, 2019)

Summary: The U.S. FDA issued a Class I recall (the most serious recall classification) for more than 4,000 Medtronic MiniMed insulin pumps after it was discovered that the controllers could wirelessly alter the insulin dose due to lack of authentication protocols on the insulin pump [36].

Impact:
- Estimated at 1 case of injury associated with unregulated insulin dosing confirmed to be unauthorized.
- Full scale device recovery, replacement, and user compensation was implemented.
- Loss of trust among customers and investors accentuated the immediate risk to brand value for Medtronic.

Root Causes:
- Lack of basic encryption or overly simplistic security on data sent and received.
- Absence of mutual authentication security for device and the controller.
- Users classified as legacy were left without a means to receive updates on firmware.

Ethical & Regulatory Implications:
- Breach of ethics concerning patient BSD and patient autonomy.
- Regulatory failure on the part of FDA in premarket review oversight neglected to account for these vulnerabilities.
- Absence of informed consent regarding the potential risk factor of wireless interfacing.

Lesson: As IoMT devices remain highly vulnerable, regulatory authorities need to enforce more rigorous premarket validation tests for cybersecurity as well as continuous monitoring for post-market activities.

7.3 Case Study 3: Singapore SingHealth Breach (2018)

Summary: In a cyber incident attributed to state-sponsored actors, SingHealth, Singapore’s largest healthcare group, suffered a data breach involving the extraction of personal information belonging to 1.5 million individuals, along with outpatient records of Prime Minister Lee Hsien Loong [37].

Impact:
- Geopolitical privacy incident at the national level.
- Creation of task force under the newly formed Cybersecurity Agency.
- Penalized with a fine of S$250,000 under Singapore’s PDPA.

Root Causes:
- Espionage phishing targeted a vulnerable endpoint.
- Moved to backend IoMT-connected devices.
- Inadequate protective infrastructure failure for inter-zone security.

Ethical & Regulatory Implications:
- Breach of confidentiality on a national scale.
- Civil discontent regarding the exploitation of sensitive data.

- Called for immediate implementations of Zero Trust frameworks.

Lessons Learned: Countries with advanced privacy frameworks are not immune to breaches if there is no strict access control and no multilayered defenses in place.

7.4 Case Study 4: St. Jude Medical Pacemaker Vulnerability (USA, 2017)

Summary: A study directed by a certain researcher revealed that some cardiac devices manufactured by St. Jude Medical can be attacked remotely to issue commands to the devices including shocking the patients or draining the battery [38].

Impact:

- Prime beneficiaries which were 465,000 patients were affected.
- FDA gave mandate for issuing a forced firmware update.
- Public erosion of trust alongside numerous lawsuits.

Root Causes:

- Authentication is not implemented at the device level.
- Use of static cryptographic keys.
- Absence of OTA (Over-the-Air) update capabilities.

Ethical and Regulatory Considerations:

- Substantial concern for the safety of patients.
- The need for preemptive "security by design" in critical life IoMT devices is evident.
- Absence of active post-deployment surveillance, and device recall processes.

Lesson: Similarly with all the critical medical devices should embed the standard security practices which already found in secure computing systems, that include encryption, firmware, authentication, and usual dynamic patching.

7.5 Synthesis of Key Takeaways

Incident	Key Vulnerability	Ethical Breach	Regulatory Failure
WannaCry (UK)	Unpatched OS	Patient harm	No mandate on patching
Medtronic (US)	No authentication	Autonomy violated	Weak FDA scrutiny
SingHealth (SG)	Endpoint compromise	Confidentiality breach	Lack of Zero Trust
St. Jude (US)	Weak firmware security	Risk to life	No OTA update requirement

Above real-world cases shown that even IoMT system which are currently in use can harbor potential problems. This is why we require strong ethics and good regulations throughout all stages from development through marketing to operation. This demonstrates the necessity of building secure firmware and implementing regular upgrades. this emphasize also that software should be audited twice: once before shipping to the market and once after it is actually in use. Ethical administration should span the product design process. Qualifications need to meet international standards should be advocated. The compliance and standard setting issues are important, though they cannot be resolved by a single move.

8. Discussion

Technological innovation, ethical accountability, and regulatory compliance must now converge in the ecosystem of the Internet of Medical Things (IoMT). As this paper has described, while IoMT brings considerable advantages to healthcare from patient monitoring and continuous interventions to tele-diagnosis, it also raises serious challenges and social risks. These risks are not only technical. Risks are obscured by the same systemic failures, namely at legal, ethical and institutional levels. This section pulls together those observations and offers a path forward in achieving a more secure and ethically responsible IoMT future.

8.1 Symptom of Technological Development Outstripping Governance of Ethics

One theme that keeps surfacing throughout the various sections based on concrete case studies, experimental research and technical assessments dealing with Ai-enabled IoMT is: the speed of ethical oversight. The pace of IoMT implementation far exceeds the pace of the ethical oversight systems devised to protect the dignity, autonomy and well-being of patient-users. Devices are deployed with little accountability, users do not understand what is done with their data, and there is little check on algorithmic bias for clinical decisions.

To counter this, the problem is not one of compliance to standards, but moving from reactive compliance and engendering the responsibility of the ethics of engineering as a proactive decision. It is important to not just consider ethics after things are marketed or established; it needs to weave throughout the whole lifecycle of product in essence from the idea and design, all the way to manufacturing, operating, and even disposal. Programs such as IEEE's Ethically Aligned Development is a good first step in making this transition [39].

8.2 Regulatory Asynchronies: Fragmentation and Double Standards

Based on our regulatory review we estimate that international law, while it limits patients in whom it works for them, offers glaring discrepancies in the laws of different countries (it limits them on the basis of being fair). For example, the strict right of resistance under GDPR is not uniformly given across EU member-states, due to varying interpretations, and is left undefined as it relates to HIPAA. Similarly, the DPDP Act in India, collects in chains or enforces stultifying state rules as juxtaposed to emerging IoMT cloud-type platforms.

More importantly, even when the laws are at play, it is often more reactive enforcement (and delayed). As in the Medtronic and SingHealth case studies, defects and vulnerabilities were only fixed after the horse had already bolted. This demonstrates an acute need for and benefit/fit for:

- Universal international standards for IoMT cybersecurity, i.e., at an international level amended from the ISO/IEC 81001 series.
- A regulatory framework that begins with "Safe by Design" which requires the manufacturers to demonstrate their security and privacy readiness prior to taking products to market.
- Automated compliance monitoring and near real-time auditing along with breach notification. General principles regarding the proof of principle concept

8.3 Proof of Concept Validation

While we see how PoC produced in the context of this investigation clearly indicated that a secure compliant IoMT system could be built at a reasonable price. Its edge-based encryption, fine-grain consent controls, and TLS communication and helped deter most attacks without breaking any laws.

Reinforcing security enables innovation rather than hindering it. If adopted everywhere this pattern industrialization, can be seen as a model for certification framework.

8.4 Evidence: Call to Action

The data reveals an alarming lack of healthcare breaches. The annual total of breached patient records has surpassed 50 million and there were over 2x ransomware incidents seen from 2020 to 2021 [23][24]. These are not just numbers—they are lives gained, disruptive upsurge in clinical practice and a consequential erosion of public trust in medical technology." Therefore, healthcare companies must:

- Consider security an enabling strategic capability, not a sunk cost.
- Use evidence and risk-adjusted budget methodologies as a vehicle for the enhancement of IoMT security.
- Establish cyber security governance boards that hold responsible for implementation and ethical compliance.
- Accept zero trust architectures as a necessary baseline, not an optional layer.

8.5 Ethical Equity & The Digital Divide

Another factor, not tied to any security concerns, is that fairness in health is another chartered dimension of IoMT deployment. Access to connected medical devices is not common from region to region, and among certain income groups and education levels. Unchecked, it is possible that IoMT could deepen the digital divide, whereby the best care only goes to those who have "digital [10]" privileges.

Therefore, as part of ethical governance, manufacturers and health systems will:

- Ensure devices are affordable and users are digitally trained;
- Engage governments when needed to support secure deployments of IoMT in underprivileged environments;
- Write their consent interfaces in local languages to further the intention to include.

8.6 Strategic Recommendations

Domain	Recommendation
Technical	Mandate encrypted firmware, secure boot, and OTA updates for all IoMT devices.
Regulatory	Create an international regulatory sandbox for IoMT to harmonize standards.
Ethical	Implement "Ethics by Design" audits as part of clinical device approval processes.
Organizational	Establish Chief Information Security Officer (CISO) roles in all healthcare settings handling IoMT.
Educational	Incorporate cybersecurity and ethics training in medical school and biomedical engineering curricula.

The discussion presents evidence that IoMT security and privacy challenges extend beyond technical limitations because they stem from fundamental ethical and regulatory and structural problems. The solution demands an interdisciplinary method which unites engineering accuracy with ethical direction and regulatory enforcement. The complete potential of IoMT can be achieved through integrating security and ethics into its development and deployment process which protects patient trust and safety and human dignity.

9. Conclusion

Medical Internet of Things technologies enable healthcare professionals to perform precision medicine alongside real-time patient monitoring. The advancement of these technologies has revealed persistent ethical concerns alongside regulatory issues and security problems which demand immediate response. The proof of concept established in this study demonstrates that a secure IoMT system can be built with privacy protection and compliance features that maintain both performance and user experience. The future of IoMT requires the collaborative effort of four pillars: regulatory harmonization, moral engineering, universal access, and institutional preparedness. This research provides a roadmap uniting empirical validation with ethical justification to support this vision.

10. Final Recommendations

- Policymakers should develop universal worldwide standards which combine IoMT cybersecurity and privacy protection.
- Engineers should embed security and ethics principles into every phase of developing IoMT devices.
- Healthcare Systems should advance their proactive auditing capabilities together with digital education programs and multi-layer security defense approaches.
- Academia should establish cross-disciplinary education programs to train future leaders who will lead ethically in technology.

We must take decisive action at this moment to build an IoMT ecosystem which delivers both excellence and security while maintaining fairness and earning trust from users.

References

[1] Markets and Markets, “IoT Medical Devices Market - Global Forecast to 2025,” 2020.

[2] Ponemon Institute, “Cost of a Data Breach Report,” IBM Security, 2023.

[3] A. Lupton, “Digital health ethics: Autonomy, consent and equity in connected care,” *J. Bioeth. Inq.*, vol. 18, no. 1, pp. 65–78, 2021.

[4] T. Cohen and M. Mello, “Big data, big tech, and protecting patient privacy,” *N. Engl. J. Med.*, vol. 381, no. 12, pp. 1011–1013, 2019.

[5] P. Lee, “Who owns my health data? A legal and ethical analysis,” *Harvard Law Rev.*, vol. 134, pp. 230–249, 2020.

[6] C. Dwork and A. Roth, “The algorithmic foundations of differential privacy,” *Found. Trends Theor. Comput. Sci.*, vol. 9, no. 3-4, pp. 211–407, 2014.

[7] J. Obermeyer et al., “Dissecting racial bias in an algorithm used to manage the health of populations,” *Science*, vol. 366, no. 6464, pp. 447–453, 2019.

[8] S. London, “Artificial intelligence and the limits of transparency,” *AI & Society*, vol. 35, pp. 283–289, 2020.

[9] L. Floridi et al., “AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations,” *Minds Mach.*, vol. 28, pp. 689–707, 2018.

[10] M. G. Wehde, “Health technology disparities and the digital divide,” *Health Aff. Blog*, Feb. 2021.

[11] European Parliament, “Regulation (EU) 2016/679 (General Data Protection Regulation),” *Official Journal of the EU*, 2016.

[12] U.S. Department of Health and Human Services, “The HIPAA Privacy Rule,” 2022.

[13] Government of India, “Digital Personal Data Protection Act, 2023,” Ministry of Electronics and IT.

[14] U.S. FDA, “Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions,” Guidance Document, 2023.

[15] European Commission, “Medical Device Regulation (MDR) 2017/745,” 2021.

[16] Office for Civil Rights, “HIPAA Breach Reporting Tool,” U.S. HHS, 2023.

[17] CISA, “Apache Log4j Vulnerability Guidance,” U.S. Cybersecurity and Infrastructure Security Agency, Dec. 2021.

[18] Ministry of Electronics and IT, India, “Data Protection Bill FAQs,” 2023.

[19] D. Leslie, “Understanding artificial intelligence ethics and safety,” *Alan Turing Institute*, 2020.

[20] ISO/IEC, “Health software and health IT systems safety, effectiveness and security—Part 1: Application of risk management,” ISO/IEC 81001-1, 2021.

[21] J. Kindervag, “Build Security Into Your Network’s DNA: The Zero Trust Network Architecture,” *Forrester Research*, 2010.

[22] OWASP Foundation, “OWASP Internet of Things Top Ten Project,” 2023.

[23] IBM Security, “Cost of a Data Breach Report 2023,” Ponemon Institute, 2023.

[24] U.S. HHS, “Breach Portal: Healthcare Data Breach Notifications,” 2024.

[25] MITRE Corporation, “Common Vulnerabilities and Exposures (CVE),” 2024.

[26] Unit 42, “Connected but Vulnerable: Cybersecurity Gaps in Medical Devices,” Palo Alto Networks, 2023.

[27] HIMSS Analytics, “State of Cybersecurity in Healthcare 2023,” Health IT Survey Report.

[28] Federal Trade Commission, “GoodRx Shares Health Data with Advertisers Without Consent,” Case No. 2022-C-0125, Jan. 2023.

[29] Deloitte Insights, “The Hidden Costs of Cyber Risk in Healthcare,” 2022.

[30] PwC, “2023 Global Digital Trust Insights: Healthcare Edition.”

[31] U.S. FDA, “Medical Device Recalls Database,” 2023.

[32] Sophos, “State of Ransomware in Healthcare 2023.”

[33] Gartner, “Measuring the Value of Security: ROSI Frameworks in Healthcare,” 2022.

[34] Frost & Sullivan, “Data Governance as a Competitive Advantage in Healthcare,” 2023.

[35] National Audit Office (UK), “Investigation: WannaCry Cyber Attack and the NHS,” 2018.

[36] U.S. FDA, “Medtronic Recalls MiniMed Insulin Pumps for Potential Cybersecurity Risks,” Recall Notice, Jul. 2019.

[37] Cyber Security Agency of Singapore, “Public Report of the Committee of Inquiry into the Cyber Attack on SingHealth,” 2019.

[38] U.S. FDA, “Firmware Update to Address Cybersecurity Vulnerabilities in St. Jude Medical Implantable Cardiac Devices,” 2017.

[39] IEEE, “Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems,” 1st ed., 2019.