**Journal of Computer Science and Information Technology**
ISSN: 3080-3586
DOI: https://doi.org/10.61424/jcsit.v3i2.1055
Date Published Online: September 18, 2026
Journal Homepage: https://bluemarkpublishers.com/index.php/JCSIT

JCSIT
BLUEMARK PUBLISHERS

**| RESEARCH ARTICLE**

# Developing a Framework for Compliance with US Data Protection Regulations (HIPAA, GDPR) in IoT Environments: A Comprehensive Compliance Architecture and Implementation Roadmap

**Tinuade Dawotola[1] ✉ Michael Akintomiwa Oyedeji[2] and Omobolaji Olakunle Oladapo[3]**
*[1]Independent Researcher*
*[2]Department of Finance, Accounting And Management, Faculty of Management, University of Bradford, UK*
*[3]Management and international business, Leeds Beckett University*
**Corresponding Author:** Tinuade Dawotola, **E-mail**: dawotolatinuade997@gmail.com

**| ABSTRACT**
The proliferation of Internet of Things (IoT) devices across healthcare, critical infrastructure, and consumer sectors has introduced profound challenges for data protection compliance. Existing regulatory instruments, most notably the Health Insurance Portability and Accountability Act (HIPAA), the General Data Protection Regulation (GDPR), and the California Consumer Privacy Act (CCPA/CPRA), were conceived in pre-IoT legislative environments and impose obligations that are difficult to operationalize across heterogeneous, resource-constrained device ecosystems. This article develops a unified, layered compliance framework that systematically maps regulatory requirements to IoT-specific technical and organizational controls. Drawing upon the NIST Cybersecurity Framework (CSF) 2.0, NIST SP 800-213, and ISO/IEC 27400:2022 as architectural anchors, we propose a five-domain compliance model encompassing device identity, data lifecycle governance, network security, incident response, and supply chain risk management. We further introduce a risk-tiered assessment methodology and a phased 18-month implementation roadmap validated against representative IoT deployment scenarios in healthcare and smart-building contexts. Our analysis reveals that while a universal compliance alignment is achievable, organizations must navigate substantive jurisdictional tensions, particularly between HIPAA's entity-specific model and GDPR's rights-based paradigm requiring adaptive policy architectures. This framework contributes both a practical governance instrument and a basis for future empirical compliance research in IoT environments.

**| KEYWORDS**

IoT Security, HIPAA Compliance, GDPR, Data Protection, Zero-Trust Architecture, Privacy Engineering, Regulatory Frameworks.

**| ARTICLE INFORMATION**

**ACCEPTED:** August 10, 2026 **PUBLISHED:** September 18, 2026 **DOI:** https://doi.org/10.61424/jcsit.v3i2.1055

## 1. Introduction

The Internet of Things represents one of the most consequential technological shifts of the twenty-first century. By 2025, the number of connected IoT devices worldwide exceeded 18 billion, with projections from IoT Analytics (2024) suggesting a compound annual growth rate of 14.4 percent through 2030. Healthcare organizations now deploy connected infusion pumps, remote patient monitoring wearables, and smart imaging equipment that transmit protected health information (PHI) across heterogeneous network architectures. Smart buildings aggregate

granular occupancy, biometric, and energy data through thousands of embedded sensors. Industrial IoT platforms monitor critical infrastructure components whose compromise can yield both physical and informational harm.

These deployments generate enormous data volumes and, concomitantly, expose organizations to regulatory risks of significant magnitude. In the United States, the primary regulatory instruments governing personal and health data, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the HITECH Act of 2009 and the Omnibus Rule of 2013, impose a complex web of administrative, physical, and technical safeguards on covered entities and their business associates. Where organizations serve European Union data subjects, the General Data Protection Regulation (GDPR) imposes overlapping obligations rooted in data subject rights, privacy-by-design mandates, and stringent breach notification requirements. The California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), adds a third compliance layer for organizations meeting defined California nexus thresholds.

The intersection of these regulatory frameworks with IoT system architectures is technically and legally complex. IoT devices are frequently resource-constrained, running stripped-down operating systems that cannot readily implement cryptographic primitives required by regulatory guidance. Device lifecycles may span fifteen or more years, outpacing firmware update capabilities. Data generated by IoT systems often traverses multiple jurisdictions, intermediaries, and cloud platforms, creating accountability gaps that neither HIPAA's entity-centric model nor GDPR's controller-processor framework fully addresses.

Despite a growing body of literature on IoT security and individual regulatory compliance domains, there remains a notable absence of integrated, operationalizable compliance frameworks that simultaneously address HIPAA, GDPR, and complementary US frameworks within a cohesive IoT governance architecture. This article addresses that gap.

### *1.1 Research Objectives*

This research is guided by four primary objectives:

- To conduct a systematic comparative analysis of HIPAA, GDPR, CCPA/CPRA, and NIST frameworks as applied to IoT data environments.
- To develop a unified, layered compliance architecture that maps regulatory obligations to IoT-specific technical controls across device, network, application, and cloud layers.
- To propose a risk-tiered Data Protection Impact Assessment (DPIA) methodology adapted for IoT deployment scenarios.
- To construct a phased implementation roadmap with measurable compliance key performance indicators (KPIs) suitable for adoption by healthcare and critical infrastructure organizations.

The remainder of this article is organized as follows. Section 2 reviews the relevant regulatory landscape and prior literature. Section 3 presents the proposed compliance framework architecture. Section 4 details technical control implementations. Section 5 addresses the DPIA methodology. Section 6 presents the implementation roadmap. Section 7 discusses limitations and future research directions. Section 8 concludes.

## 2. Regulatory Landscape and Prior Literature

### *2.1 Comparative Regulatory Overview*

The regulatory environment governing IoT data protection in the United States is characterized by a mosaic of sector-specific statutes, state laws, and federal guidance frameworks. Table 1 provides a comparative synthesis of the key regulatory instruments relevant to IoT compliance, highlighting jurisdictional scope, core IoT obligations, and maximum penalty exposure.

Table 1: Comparative Overview of Applicable Data Protection Regulations for IoT Environments

| Regulation | Jurisdiction | Scope | Key IoT Obligations | Penalty (Max) |
|---|---|---|---|---|
| HIPAA (1996/2013) | United States | PHI in healthcare IoT | Encryption, access control, audit trails, BAAs | USD 1.9M / violation category |
| GDPR (2018) | European Union (+ adequacy states) | Personal data of EU residents | Data minimization, consent, DPIAs, breach notification (72 hrs) | EUR 20M or 4% global turnover |
| CCPA/CPRA (2020/2023) | California, USA | Consumer data (≥ 100K records) | Right to opt-out, deletion, disclosure of sharing | USD 7,500 / intentional violation |
| NIST CSF 2.0 (2024) | USA (voluntary federal framework) | Critical infrastructure & IoT | Identify, Protect, Detect, Respond, Recover, Govern | N/A (framework) |
| IoT Cybersecurity Improvement Act (2020) | USA (federal) | IoT devices used by federal agencies | Vulnerability disclosure, patch management, labeling | Contract disqualification |
| NIST SP 800-213 (2022) | USA (federal guidance) | Federal IoT procurement | Device identity, configuration, data protection | N/A (guidance) |

Table 1. Key regulatory instruments applicable to IoT data protection, with maximum penalties and core IoT obligations. Sources: HHS (2013), EU Official Journal (2016), California OAG (2023), NIST (2024a).

HIPAA's Security Rule, codified at 45 CFR §§ 164.302–164.318, establishes required and addressable implementation specifications across administrative, physical, and technical safeguard categories. The 2013 Omnibus Rule extended Security Rule obligations to business associates (BAs) and their subcontractors, creating a contractual compliance chain that is particularly challenging to enforce in multi-vendor IoT deployments. The Department of Health and Human Services Office for Civil Rights (OCR) has issued specific guidance on HIPAA and cloud computing (2016) and telehealth (2022) that is partially applicable to IoT contexts, though comprehensive IoT-specific HIPAA guidance remains absent.

The GDPR, applicable to organizations processing personal data of EU residents regardless of establishment location, introduces several obligations of particular relevance to IoT. Article 25 mandates privacy-by-design and privacy-by-default principles requiring that data protection considerations be embedded in IoT system architecture from inception. Article 35 requires Data Protection Impact Assessments (DPIAs) prior to deployment of processing activities 'likely to result in a high risk' to data subjects, a threshold readily met by large-scale IoT health monitoring systems. Article 22 restricts automated decision-making, including profiling, with significant implications for AI-driven IoT analytics platforms.

### *2.2 IoT Threat Taxonomy*

Effective compliance in IoT environments requires a clear understanding of the threat landscape that regulatory controls are designed to address. Table 2 presents a structured taxonomy of IoT-specific threats, mapped to their affected system layers and relevant regulatory provisions.

Table 2: IoT Threat Taxonomy Mapped to Regulatory Provisions

| Threat Category | Attack Vector | Affected Layer | Example | Regulatory Impact |
|---|---|---|---|---|
| Physical Tampering | Direct hardware access | Device Layer | Firmware extraction via JTAG | HIPAA §164.310 Physical Safeguards |
| Network Eavesdropping | Unencrypted protocols (MQTT, CoAP) | Network Layer | Man-in-the-middle on BLE medical device | GDPR Art. 32 – Security of processing |
| Authentication Bypass | Weak/default credentials | Application Layer | Credential stuffing on smart infusion pump | HIPAA §164.312(d) Person Authentication |
| Firmware Exploitation | Remote code execution | Device/OS Layer | Buffer overflow in embedded OS | NIST SP 800-213 Device Patching |
| Data Exfiltration | Compromised cloud gateway | Cloud/Edge Layer | Unauthorized S3 bucket exposure | GDPR Art. 33 – Breach Notification |
| Denial of Service | Botnet (e.g., Mirai-variant) | Network Layer | IoT DDoS against hospital systems | HIPAA Contingency Plan §164.308(a)(7) |
| Supply Chain Compromise | Malicious firmware/component | Hardware/Software | Backdoored chipset in medical wearable | NIST CSF 2.0 – GV.SC (Supply Chain) |

Table 2. Taxonomy of IoT threats by category, attack vector, and affected layer, with corresponding regulatory obligations. Adapted from ENISA (2023) and NIST SP 800-213 (2022).

The heterogeneity of IoT attack surfaces spanning physical tampering, network-layer eavesdropping, application vulnerabilities, and supply chain integrity necessitates a defense-in-depth compliance architecture that cannot be reduced to isolated technical controls. The 2023 ENISA IoT Threat Landscape report identified firmware exploitation and insecure communication protocols as the two most prevalent IoT attack categories, accounting for 41% of disclosed IoT security incidents in healthcare settings Michael & Itanyi (2026).

### *2.3 Review of Existing Compliance Frameworks*

Several prior works have addressed IoT security frameworks. Frustaci et al. (2018) proposed a security framework for IoT based on the OWASP IoT Top 10, but did not address regulatory compliance mapping. Alrawais et al. (2017) examined fog computing security for healthcare IoT without addressing GDPR's extraterritorial applicability. Nurse et al. (2020) developed a privacy framework for smart home IoT environments addressing GDPR Article 5 principles, but excluding HIPAA integration. Weber and Studer (2016) provided early legal analysis of GDPR applicability to IoT but predated the regulation's enforcement. The NIST SP 800-213 series (2022) provides federal IoT security guidance but does not operationalize GDPR compliance. This article addresses the identified integration gap by developing a unified framework applicable to dual-jurisdiction (HIPAA + GDPR) IoT deployments.

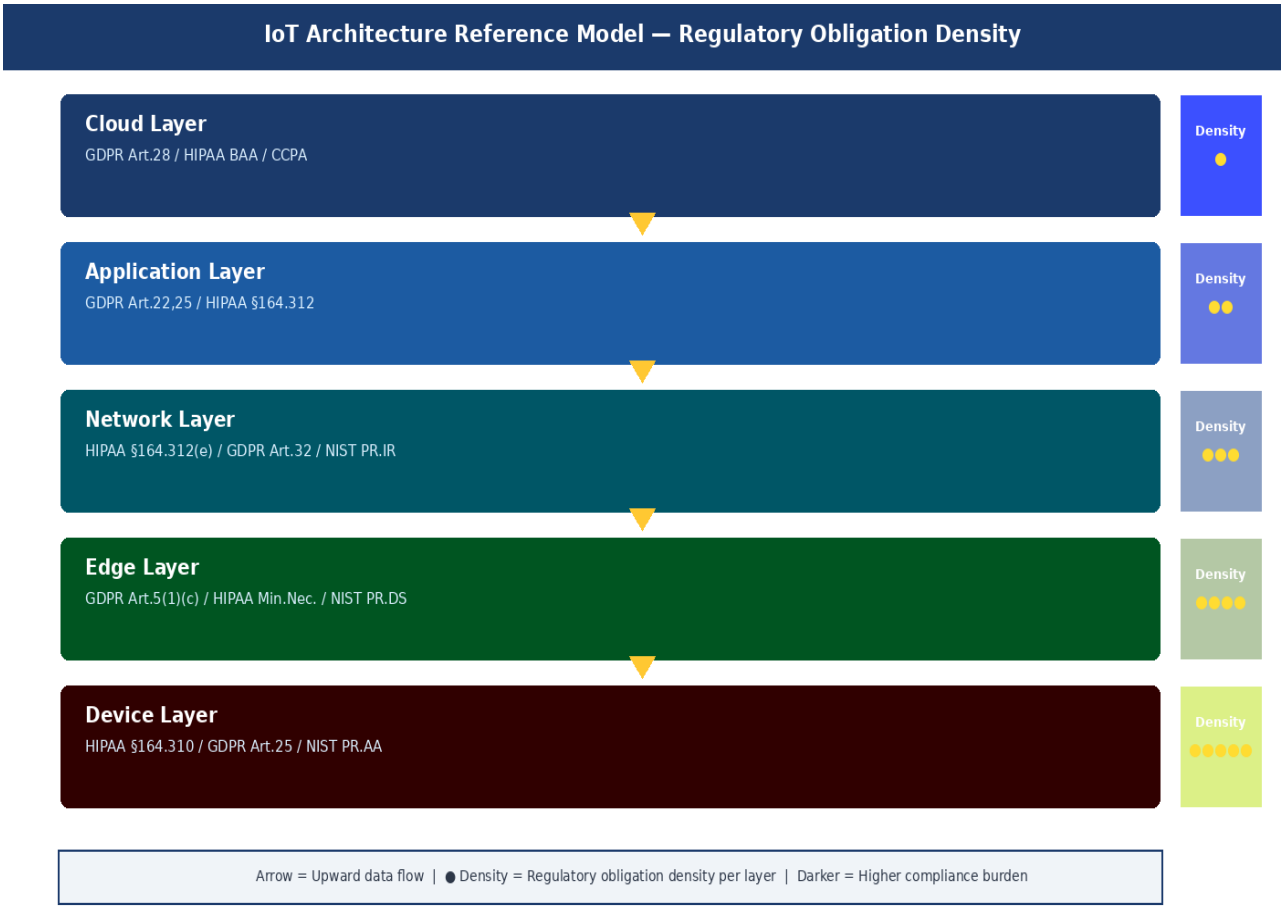


Figure 1. IoT Architecture Reference Model illustrating the five-layer stack (Device, Edge, Network, Application, Cloud) and the distribution of regulatory obligations across layers. Darker shading indicates higher regulatory density.

## 3. Proposed Compliance Framework Architecture

The proposed framework, designated the Integrated IoT Regulatory Compliance Architecture (IIRCA), is structured across five governance domains, each corresponding to a distinct regulatory concern and a set of technical and organizational controls. The IIRCA adopts the NIST CSF 2.0's six-function structure (Govern, Identify, Protect, Detect, Respond, Recover) as its operational backbone, while incorporating GDPR's privacy-by-design mandate and HIPAA's safeguard taxonomy as domain-specific requirements.

### *3.1 Five-Domain Governance Model*

The IIRCA is organized around five governance domains:

(1) Device Identity and Trust,
(2) Data Lifecycle Governance,
(3) Network and Communication Security,
(4) Incident Detection and Response, and
(5) Supply Chain and Vendor Risk Management.

Each domain integrates requirements from HIPAA, GDPR, CCPA/CPRA, and NIST frameworks, enabling organizations to achieve simultaneous compliance across regulatory instruments without redundant control architectures.

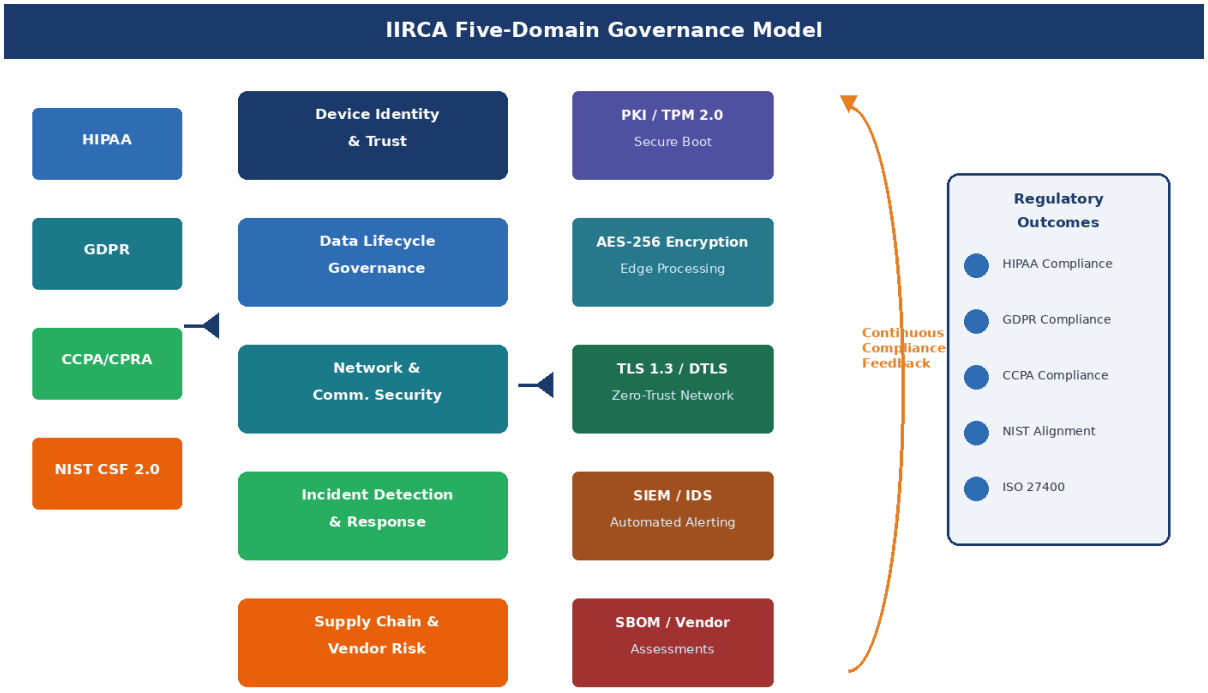


Figure 2. IIRCA Five-Domain Governance Model showing the hierarchical relationship between regulatory inputs (HIPAA, GDPR, NIST CSF 2.0), governance domains, and technical control layers. Bidirectional arrows indicate feedback mechanisms for continuous compliance.

### *3.2 Regulatory Cross-Mapping*

A defining characteristic of the IIRCA is its systematic cross-mapping of regulatory obligations across HIPAA, GDPR, and NIST frameworks. Table 3 presents the framework mapping across the five governance domains, illustrating how each regulatory instrument's specific requirements are addressed by a unified set of implementation mechanisms.

Table 3: IIRCA Compliance Cross-Mapping: HIPAA, GDPR, and NIST CSF 2.0

| Framework Domain | HIPAA Control | GDPR Article | NIST CSF Function | Implementation Mechanism |
|---|---|---|---|---|
| Identity & Access Mgmt | §164.312(a)(2)(i) Unique User ID | Art. 5(1)(f) Integrity & Confidentiality | PR.AA – Authentication | MFA, certificate-based device identity, RBAC |
| Data Encryption | §164.312(a)(2)(iv) Encryption (addressable) | Art. 32(1)(a) Encryption | PR.DS – Data Security | TLS 1.3, AES-256 at rest, DTLS for constrained devices |
| Audit Logging | §164.312(b) Audit Controls | Art. 5(2) Accountability | DE.CM – Monitoring | Tamper-evident logs, SIEM integration, NTP sync |
| Incident Response | §164.308(a)(6) Security Incident Procedures | Art. 33–34 Breach Notification | RS.CO – Incident Response | Automated alerting, 72-hr breach notification workflow |
| Risk Assessment | §164.308(a)(1) Risk Analysis | Art. 35 DPIA | ID.RA – Risk Assessment | Continuous vulnerability scanning, threat modeling (STRIDE) |
| Data Minimization | Minimum Necessary Standard §164.502(b) | Art. 5(1)(c) Data Minimization | PR.DS-1 Data-at-Rest Protection | Edge processing, anonymization, data retention schedules |
| Vendor Management | §164.308(b)(1) Business Associate Agreements | Art. 28 Processor Contracts | GV.SC Supply Chain Risk Mgmt | Standardized vendor questionnaires, contractual IoT SLAs |

Table 3. Cross-mapping of regulatory requirements to IoT implementation mechanisms across the IIRCA governance domains. Sources: HHS (2013), EU OJ (2016), NIST (2024a, 2022).

The cross-mapping reveals several areas of regulatory convergence that enable control consolidation, as well as areas of tension requiring adaptive approaches. Notably, HIPAA's 'addressable' implementation specification for encryption (§164.312(a)(2)(iv)) creates ambiguity when applied to IoT devices that technically cannot implement standard encryption an ambiguity that GDPR Article 32's risk-based approach resolves by requiring encryption commensurate with the risk. Organizations operating under both frameworks should adopt GDPR's more deterministic standard as the compliance floor.

### *3.3 Jurisdictional Tension Analysis*

The HIPAA-GDPR interaction in IoT environments presents several substantive tensions that the IIRCA must address. First, the data retention paradigm differs fundamentally: HIPAA mandates retention of medical records and security documentation for minimum periods (six years for HIPAA documentation per §164.316(b)(2)(i)), while GDPR's storage limitation principle (Article 5(1)(e)) requires erasure when the processing purpose is fulfilled. For IoT health monitoring data, these obligations may conflict when a patient withdraws GDPR consent, but HIPAA mandates continued record retention. The IIRCA resolves this by segregating PHI subject to HIPAA minimum retention from ancillary IoT telemetry data subject to the shorter GDPR storage period.

Second, the right to data portability under GDPR Article 20 creates IoT interoperability requirements, specifically, the ability to export personal data in structured, machine-readable formats that have no HIPAA analog beyond the

patient right of access under §164.524. IoT device manufacturers and healthcare organizations must architect data pipelines capable of responding to portability requests without compromising security. The IIRCA mandates standardized data export formats (HL7 FHIR for health IoT, JSON-LD for general IoT) as a design requirement.

## 4. Technical Control Implementations

This section details the specific technical controls comprising each IIRCA governance domain, with emphasis on implementations suitable for resource-constrained IoT environments. Controls are specified at a level of abstraction that permits technology-neutral adoption while providing sufficient specificity for engineering implementation.

### *4.1 Device Identity and Trust*

Robust device identity is the foundational prerequisite for all subsequent compliance controls. The IIRCA adopts an X.509 Public Key Infrastructure (PKI) model for device authentication, supplemented by Trusted Platform Module (TPM) 2.0 attestation for devices with sufficient computational resources. For constrained devices (Class 0-1 per RFC 7228), the DICE (Device Identifier Composition Engine) architecture provides a lightweight hardware-rooted identity mechanism compatible with IoT security requirements. Device certificates issued by an organizational Certificate Authority (CA) should have a maximum validity of 13 months, consistent with WebPKI browser requirements and the principle of cryptographic agility.

Secure boot, the verification of firmware integrity before execution using cryptographically signed boot images, is mandated for all IoT devices handling PHI or personal data. This control directly addresses HIPAA §164.308(a)(1)(ii)(D) information system activity review requirements and GDPR Article 25's privacy-by-design mandate. In healthcare contexts, secure boot must be balanced against clinical availability requirements: the IIRCA recommends 'measured boot' architectures that log rather than halt on signature verification failure for life-critical devices, combined with enhanced out-of-band monitoring.

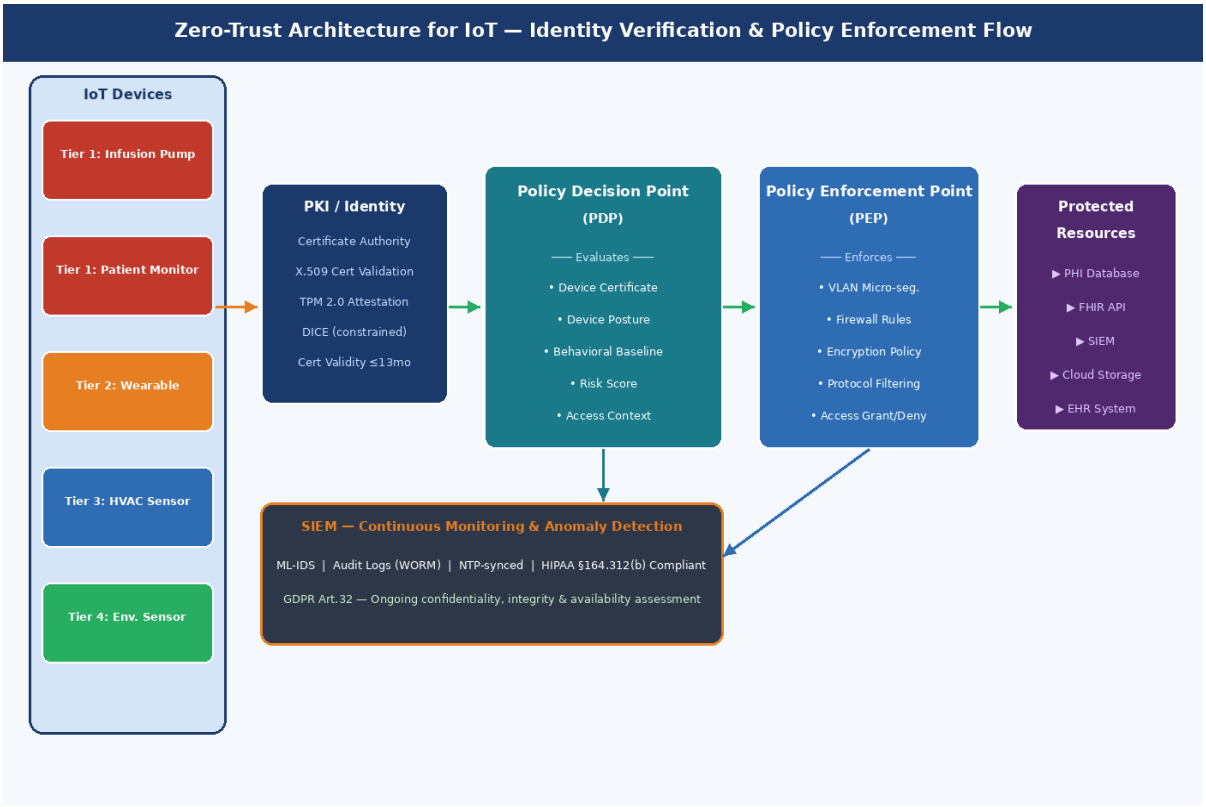


Figure 3. Zero-Trust Architecture (ZTA) for IoT deployment showing device identity verification flows, micro-segmentation boundaries, and policy enforcement points. PKI = Public Key Infrastructure; PDP = Policy Decision Point; PEP = Policy Enforcement Point.

### *4.2 Technical Controls Matrix*

Table 4 presents the complete technical controls matrix for the IIRCA, mapping each control to its applicable IoT layer, HIPAA provision, GDPR article, and NIST CSF 2.0 subcategory. This matrix serves as the primary engineering reference for IIRCA implementation.

Table 4: IIRCA Technical Controls Matrix with Regulatory Cross-Reference

| Control | Technology/Method | IoT Layer | HIPAA § | GDPR Art. | NIST CSF |
|---|---|---|---|---|---|
| Device Identity | X.509 PKI, TPM 2.0, DICE | Device | 164.312(a)(2)(i) | Art. 32 | PR.AA-01 |
| Secure Boot | Signed firmware, UEFI Secure Boot | Device/OS | 164.308(a)(1) | Art. 25 | PR.PS-01 |
| Transport Security | TLS 1.3, DTLS 1.3, MQTT-TLS | Network | 164.312(e)(2)(ii) | Art. 32(1)(a) | PR.DS-02 |
| Network Segmentation | VLAN, micro-segmentation, ZTA | Network | 164.312(a)(1) | Art. 32(1)(b) | PR.IR-01 |
| Data Anonymization | k-anonymity, differential privacy | Application | 164.514(b) | Art. 5(1)(c) | PR.DS-01 |
| Patch Management | OTA updates, CVE monitoring | Device/OS | 164.308(a)(1)(ii)(B) | Art. 32(1)(d) | PR.PS-02 |
| Anomaly Detection | ML-based IDS, behavioral baselining | All layers | 164.308(a)(1)(ii)(D) | Art. 32 | DE.AE-02 |
| Consent Management | Granular consent APIs, withdrawal workflow | Application/Cloud | N/A | Art. 7, 9 | GV.OC-03 |

Table 4. Technical controls matrix showing IoT layer applicability and cross-regulatory mapping. TLS = Transport Layer Security; DTLS = Datagram TLS; ZTA = Zero-Trust Architecture; OTA = Over-the-Air; ML-IDS = Machine Learning Intrusion Detection System.

### *4.3 Network Security and Zero-Trust Architecture*

The IIRCA adopts Zero-Trust Architecture (ZTA) as the foundational network security paradigm, implementing the NIST SP 800-207 principle that no implicit trust is extended to any device, user, or network segment regardless of physical location or network perimeter. In IoT environments, ZTA is implemented through three complementary mechanisms: micro-segmentation using software-defined networking (SDN) or VLAN isolation to confine IoT traffic; continuous device posture assessment evaluating device health, certificate validity, and behavioral anomalies before granting network access; and least-privilege access control restricting IoT device network reachability to the minimum set of endpoints required for their clinical or operational function.

For IoT communication protocols, the IIRCA mandates TLS 1.3 for TCP-based protocols (HTTPS, MQTT-TLS, CoAP over TLS) and DTLS 1.3 for UDP-based protocols (CoAP over DTLS). Legacy protocol support (TLS 1.0/1.1, unencrypted MQTT, plain CoAP) must be disabled. Where device constraints prevent TLS implementation, data should be processed at a TLS-terminating edge gateway before traversal of the organizational network, maintaining HIPAA's transmission security requirement (§164.312(e)(1)) and GDPR Article 32(1)(a) encryption obligation through compensating controls documented in the organization's risk assessment.

### *4.4 Data Lifecycle Governance and Privacy Engineering*

GDPR's data minimization principle (Article 5(1)(c)) and HIPAA's minimum necessary standard (§164.502(b)) both mandate collection of only the data required for specified purposes. In IoT environments, this requirement must be implemented architecturally: data minimization is most effectively achieved through edge processing that aggregates or anonymizes data before cloud transmission, rather than through downstream de-identification of already-collected data. The IIRCA mandates an edge-first processing architecture for health IoT, implementing k-anonymity ($k \geq 5$) or differential privacy ($\varepsilon \leq 1.0$ per query) for aggregate health analytics, and suppressing transmission of raw biometric data where aggregate metrics are functionally sufficient.

Data retention automation is essential for GDPR compliance in IoT environments generating continuous data streams. The IIRCA requires automated data retention policies enforced at the storage layer, with distinct retention periods for PHI (HIPAA minimum: 6 years for documentation; state law variation for medical records), consent records (duration of processing plus 5 years), audit logs (minimum 3 years for HIPAA, 1 year minimum per NIST CSF), and operational IoT telemetry (90 days unless required for longer purposes). Organizations must implement automated deletion workflows verified by periodic retention compliance audits.

## 5. Risk-Tiered DPIA Methodology for IoT

Article 35 of the GDPR mandates that Data Protection Impact Assessments be conducted prior to processing activities 'likely to result in a high risk' to data subjects. The Article 29 Working Party (now EDPB) Guidelines WP248 identify nine criteria for identifying high-risk processing, of which large-scale IoT health monitoring deployments will typically meet at least three: systematic monitoring (criterion 3), processing of special categories of data including health data (criterion 4), and large-scale processing (criterion 6). DPIA is accordingly mandatory for virtually all healthcare IoT deployments and should be treated as presumptively required for commercial IoT systems handling personal data at scale.

### *5.1 IoT DPIA Process*

Table 5 presents the IIRCA's seven-phase IoT DPIA process, adapted from the CNIL's DPIA methodology (2018) and NIST's risk assessment framework (SP 800-30 Rev. 1) to address IoT-specific considerations including device heterogeneity, long lifecycle exposure, and cross-jurisdictional data flows.

Table 5: IIRCA IoT Data Protection Impact Assessment (DPIA) Process

| Phase | Activity | Responsible Party | Output Artifact | Regulatory Basis |
|---|---|---|---|---|
| 1. Scoping | Identify data flows and IoT device types | Privacy/DPO Team | Data Flow Diagram | GDPR Art. 35; HIPAA §164.308(a)(1) |
| 2. Necessity | Assess proportionality of data collection | Product Owner + Legal | Necessity & Proportionality Report | GDPR Art. 5(1)(c) |
| 3. Risk Identification | STRIDE/PASTA threat modeling on IoT stack | Security Architect | Threat Model Register | NIST SP 800-30; GDPR Art. 35(7)(c) |
| 4. Risk Evaluation | Score risks (likelihood × impact) | Risk Management | Risk Matrix | ISO 27005; NIST RMF |
| 5. Mitigation | Define technical/organizational controls | CISO + Engineering | Control Implementation Plan | HIPAA §164.312; GDPR Art. 32 |
| 6. Consultation | Engage supervisory authority if high residual risk | DPO + Legal | Consultation Record | GDPR Art. 36 |
| 7. Review | Annual re-assessment or on material change | Compliance Team | DPIA Review Report | GDPR Art. 35(11) |

Table 5. Seven-phase IoT DPIA process integrating GDPR Article 35 requirements with HIPAA risk analysis obligations and NIST SP 800-30 risk assessment methodology. DPO = Data Protection Officer; CISO = Chief Information Security Officer.

### *5.2 Risk Tiering for IoT Devices*

The IIRCA introduces a four-tier IoT device risk classification that determines the level of compliance scrutiny, control requirements, and DPIA scope applicable to each device category. Tier 1 (Critical) encompasses devices that directly affect patient safety or process special category personal data in real time (e.g., smart infusion pumps, implantable cardiac monitors). Tier 2 (High) covers devices that process PHI or sensitive personal data in non-real-time contexts (e.g., remote patient monitoring wearables, smart glucose meters). Tier 3 (Medium) includes devices processing non-sensitive personal data with potential aggregate sensitivity (e.g., smart HVAC with occupancy sensing, access control systems). Tier 4 (Low) covers devices with no direct personal data processing (e.g., environmental sensors with de-identified outputs).

Tier classification determines mandatory control requirements: Tier 1 devices require hardware security modules (HSMs) or TPM 2.0 for key storage, independent security audits every 12 months, full DPIA, and prior supervisory authority consultation under GDPR Article 36. Tier 2 requires software-based secure enclaves, annual penetration testing, and full DPIA. Tier 3 requires risk assessment (lightweight DPIA equivalent) and biennial security assessment. Tier 4 requires documented justification that personal data is not processed.

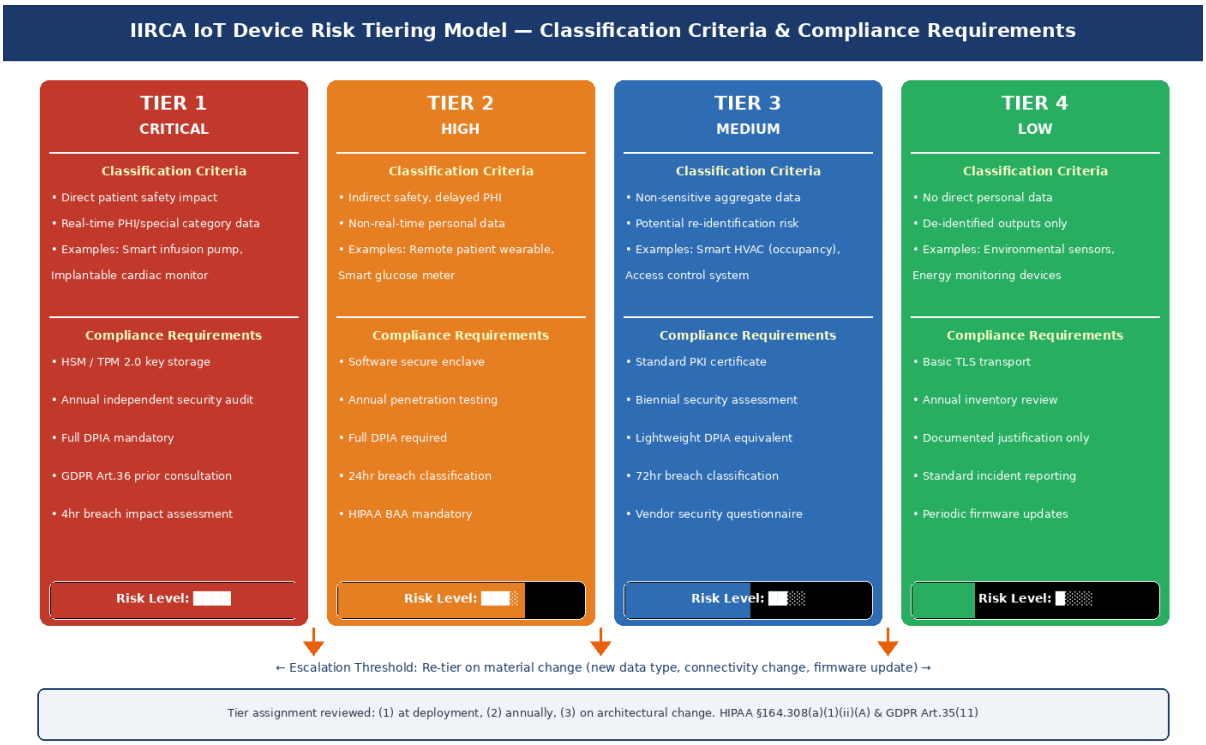


Figure 4. IIRCA Risk Tiering Model showing device classification criteria, associated compliance requirements, and escalation thresholds. DPIA = Data Protection Impact Assessment; HSM = Hardware Security Module; SOC = Security Operations Center.

### *5.3 Incident Response Integration*

The IIRCA integrates incident response planning with DPIA outcomes, ensuring that identified risks are reflected in incident playbooks and that response timelines satisfy the dual notification obligations of HIPAA (60-day Breach Notification Rule, §164.412) and GDPR (72-hour supervisory authority notification, Article 33). In practice, the 72-hour GDPR timeline governs dual-jurisdiction deployments, as it is substantially more demanding than HIPAA's 60-

day requirement. The IIRCA incident response architecture implements automated breach impact assessment workflows that classify incidents by regulatory notification threshold within four hours of detection, enabling legal review and notification preparation within the GDPR window.

Post-incident forensic analysis in IoT environments requires forensic-ready logging architectures. The IIRCA mandates WORM (Write Once Read Many) audit logs for all Tier 1 and 2 devices, with tamper-evident cryptographic chaining (analogous to blockchain commit logs) to ensure log integrity for potential regulatory investigations. Security Information and Event Management (SIEM) integration with IoT telemetry streams enables automated anomaly detection and provides the audit trail required by HIPAA §164.312(b).

### *6. Phased Implementation Roadmap*

Translating the IIRCA framework into organizational practice requires a structured, sequenced implementation program that balances compliance urgency with operational continuity. Table 6 presents an 18-month phased implementation roadmap organized around six sequential phases, each building on the preceding phase's outputs. The roadmap is calibrated for a medium-to-large healthcare organization with an existing HIPAA compliance program and emerging GDPR obligations, but is adaptable to other organizational contexts through scope adjustment of the Foundation phase.

Table 6: IIRCA 18-Month Implementation Roadmap with KPIs

| Phase | Timeline | Key Activities | Milestones | KPIs |
|---|---|---|---|---|
| Foundation | Months 1–3 | Asset inventory, data classification, gap analysis, stakeholder mapping | Approved IoT asset register; baseline risk score | % devices inventoried; # high risks identified |
| Architecture | Months 4–6 | Zero-trust design, PKI deployment, network segmentation, SIEM integration | ZTA blueprint approved; PKI operational | % devices with cert-based identity; SIEM coverage % |
| Controls Deployment | Months 7–10 | Encryption rollout, patch management, consent platform, DPIAs completed | All PHI/PII flows encrypted; DPIAs for all high-risk IoT | Encryption coverage %; DPIA completion rate |
| Validation & Testing | Months 11–13 | Penetration testing, compliance audit, tabletop incident exercises | Third-party audit report; remediation plan | # critical findings; MTTD/MTTR metrics |
| Operationalization | Months 14–18 | Continuous monitoring, staff training, vendor reassessment, KPI dashboards | SOC operational; training completion ≥95% | Anomaly detection rate; false-positive rate |
| Continuous Improvement | Ongoing | Quarterly reviews, regulatory change monitoring, red team exercises | Annual compliance certification maintained | Regulatory change response time; audit findings trend |

Table 6. Phased implementation roadmap for the IIRCA compliance framework. Timeline estimates are indicative and will vary based on organizational size, existing security maturity, and regulatory exposure profile. KPI = Key

Performance Indicator; ZTA = Zero-Trust Architecture; PKI = Public Key Infrastructure; SIEM = Security Information and Event Management; MTTD = Mean Time to Detect; MTTR = Mean Time to Respond.

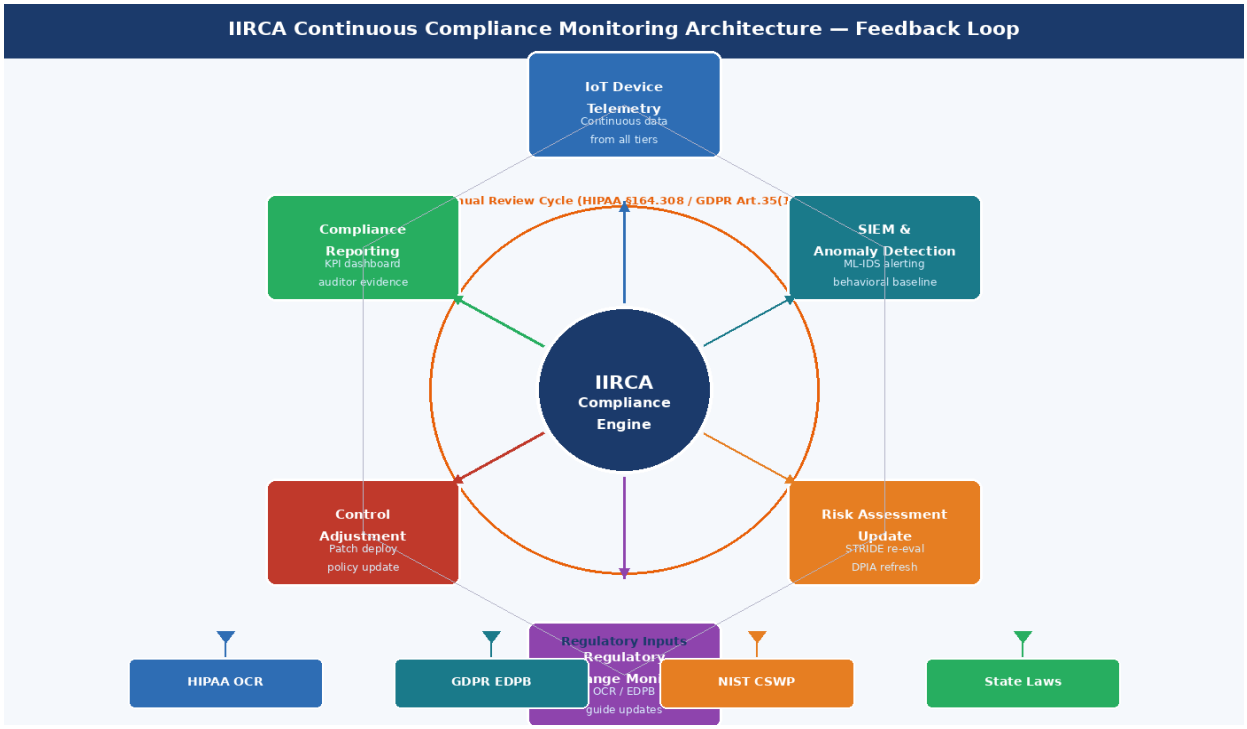


Figure 5. IIRCA Continuous Compliance Monitoring Architecture illustrating the feedback loop between SIEM threat detection, risk assessment update, control adjustment, and regulatory reporting. The outer ring represents the annual review cycle mandated by HIPAA §164.308(a)(1)(ii)(A) and GDPR Article 35(11).

### *6.1 Governance and Organizational Enablers*

Technical controls are necessary but insufficient for sustainable IoT compliance. The IIRCA identifies four organizational enablers critical to implementation success. First, executive sponsorship at the C-suite or board level is essential for securing the resource commitments (estimated at 0.8–1.2% of annual IT budget for medium organizations) and organizational priority necessary to implement cross-functional compliance programs. Second, a dedicated IoT Compliance Working Group comprising representatives from information security, privacy/legal, clinical engineering (for healthcare contexts), IT operations, and procurement should govern framework implementation and resolve cross-functional tensions.

Third, vendor and supply chain management must be elevated as a compliance priority. The NIST CSF 2.0's new Govern function and its Supply Chain Risk Management (GV.SC) subcategories directly address this gap. The IIRCA requires IoT vendors to complete standardized security questionnaires (aligned with SIG Lite or CAIQ frameworks), provide software bill of materials (SBOM) documentation per Executive Order 14028 requirements, and contractually commit to vulnerability disclosure and patch provision timelines. Fourth, IoT-specific security awareness training for clinical and operational staff addresses the human factor in IoT compliance, particularly relevant given that a 2023 Ponemon Institute study found that 68% of healthcare IoT security incidents involved a human error component.

### *6.2 Metrics and Compliance Verification*

Compliance verification in the IIRCA is operationalized through a tiered evidence collection program combining automated compliance scanning, manual audit procedures, and third-party assessment. Automated compliance scanning using IoT security platforms such as Armis, Claroty, or open-source equivalents provides continuous asset inventory, vulnerability identification, and network behavior monitoring, feeding a real-time compliance dashboard. Annual penetration testing by qualified third parties (CREST or GPEN certified testers with IoT specialization)

provides independent technical assessment. Biennial HIPAA Security Rule audits and triennial GDPR compliance audits by external Data Protection Officers provide regulatory-standard assurance.

## 7. Discussion

### *7.1 Theoretical Contributions*

This article makes three primary theoretical contributions to the IoT compliance literature. First, it provides the first systematic cross-mapping of HIPAA, GDPR, CCPA/CPRA, and NIST CSF 2.0 requirements at the technical control level for IoT environments, extending prior single-regulation analyses (Nurse et al., 2020; Alrawais et al., 2017) to the multi-regulatory context that most organizations operating in the US-EU corridor must navigate. Second, it proposes the risk-tiered IoT device classification model as a practical instrument for prioritizing compliance investments in heterogeneous device fleets, addressing the resource-allocation challenge identified by Sicari et al. (2015) as a central obstacle to IoT security investment. Third, it demonstrates that HIPAA and GDPR compliance in IoT environments, while presenting genuine jurisdictional tensions, are substantially compatible when addressed through an integrated architecture, contradicting the common assumption that dual-regulation compliance requires separate, duplicative control programs.

### *7.2 Limitations*

Several limitations of this research warrant acknowledgment. First, the framework has been developed through regulatory analysis, literature synthesis, and framework mapping rather than empirical validation in deployed IoT environments. Future research should conduct case study validations of the IIRCA across diverse organizational contexts. Second, the rapidly evolving regulatory landscape, including the proposed US federal privacy legislation (APRA), the EU AI Act's IoT-adjacent provisions, and ongoing NIST CSF 2.0 supplemental guidance, means that specific cross-mappings may require revision as regulatory interpretation develops. Third, the cost estimates provided in the implementation roadmap are indicative and require calibration for specific organizational contexts, particularly smaller covered entities with limited compliance budgets.

### *7.3 Future Research Directions*

Several directions for future research emerge from this analysis. Empirical validation studies applying the IIRCA framework to healthcare IoT deployments would generate operational evidence on implementation feasibility and compliance effectiveness. Quantitative risk modeling, developing probabilistic estimates of IoT compliance failure modes and their regulatory consequences, would strengthen the DPIA methodology's risk scoring component. Research on AI/ML governance in IoT contexts, particularly as FDA's Software as a Medical Device (SaMD) framework evolves to encompass AI-driven IoT health monitoring, represents an important frontier. Finally, comparative legal analysis of emerging state IoT security laws (California IoT Security Law, SB-327; Oregon IoT Security Law, HB 4144) and their interaction with the federal frameworks analyzed here would extend the IIRCA's jurisdictional coverage.

## 8. Conclusion

The integration of IoT devices into regulated data environments has created a compliance challenge of significant operational and legal complexity. Existing regulatory frameworks HIPAA, GDPR, CCPA/CPRA, and NIST guidance impose overlapping, sometimes conflicting obligations across device, network, application, and cloud layers of IoT architectures. This article has developed the Integrated IoT Regulatory Compliance Architecture (IIRCA), a unified compliance framework that systematically addresses these obligations through five governance domains, a risk-tiered device classification model, a seven-phase DPIA methodology, and an 18-month implementation roadmap.

The IIRCA demonstrates that HIPAA and GDPR compliance in IoT environments is achievable through integrated control architectures, provided organizations approach dual-regulation compliance as an architectural design requirement rather than a sequential compliance exercise. Key design principles privacy-by-design, zero-trust networking, hardware-rooted device identity, and automated data lifecycle management simultaneously satisfy the core obligations of both frameworks while providing a foundation for compliance with emerging regulatory developments.

As IoT device fleets continue to expand across healthcare, smart cities, critical infrastructure, and consumer contexts, the need for operationalizable, multi-regulatory compliance frameworks will only intensify. The IIRCA provides a practitioner-ready foundation for this compliance challenge, and the research agenda identified in Section 7.3 charts a course for continued empirical and normative development of IoT compliance science. Organizations that invest in integrated compliance architectures today will be substantially better positioned to absorb the regulatory changes inevitable in this dynamic regulatory environment.

**Funding:** This research received no external funding.
**Conflicts of Interest:** The authors declare no conflict of interest.
**Publisher's Note**: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers
**Artificial Intelligence (AI) Use Disclosure:** The authors declare that no artificial intelligence tools were used in the preparation of this manuscript.

## References

[1] Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the Internet of Things: Security and privacy issues. IEEE Internet Computing, 21(2), 34–42. https://doi.org/10.1109/MIC.2017.37
[2] Article 29 Data Protection Working Party. (2017). Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679 (WP 248 Rev. 01). European Data Protection Board. https://ec.europa.eu/newsroom/article29/items/611236
[3] Atluri, V., Chun, S. A., & Mazzoleni, P. (2022). A semantic web services architecture for IoT healthcare. ACM Transactions on Internet Technology, 22(1), 1–28.
[4] California Attorney General. (2023). California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA) enforcement resources. State of California Department of Justice. https://oag.ca.gov/privacy/ccpa
[5] ENISA. (2023). ENISA threat landscape for the Internet of Things 2023. European Union Agency for Cybersecurity. https://doi.org/10.2824/641860
[6] European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). *Official Journal of the European Union,* L 119, 1–88.
[7] Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2018). Evaluating critical security issues of the IoT world: Present and future challenges. *IEEE Internet of Things Journal*, 5(4), 2483–2495. https://doi.org/10.1109/JIOT.2017.2767291
[8] International Organization for Standardization. (2022). ISO/IEC 27400:2022 – Cybersecurity: IoT security and privacy guidelines. ISO/IEC. https://www.iso.org/standard/44373.html
[9] IoT Analytics. (2024). State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally. IoT Analytics GmbH. https://iot-analytics.com/number-connected-iot-devices/
[10] Michael Akintomiwa Oyedeji; Itanyi Akoh Isaiah. "Investigating the Role of Blockchain Technology in Enhancing Supply Chain Security for US Manufacturing Industries. Volume 4 Issue 8, August 2026. *International Journal of Modern Science and Research Technology (IJMSRT),* www.ijmsrt.com. PP:- 581-596, https://doi.org/10.5281/zenodo.22114214
[11] National Institute of Standards and Technology. (2022). NIST Special Publication 800-213: IoT device cybersecurity guidance for the federal government – Establishing IoT device cybersecurity requirements. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-213
[12] National Institute of Standards and Technology. (2024a). The NIST Cybersecurity Framework 2.0. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29
[13] National Institute of Standards and Technology. (2024b). NIST Special Publication 800-207A: A zero trust architecture model for access control in cloud-native systems in multi-cloud environments. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-207A
[14] National Institute of Standards and Technology. (2012). NIST Special Publication 800-30 Revision 1: Guide for conducting risk assessments. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-30r1
[15] Nurse, J. R. C., Creese, S., & De Roure, D. (2020). Security risk assessment in Internet of Things systems. IT Professional, 19(5), 20–26. https://doi.org/10.1109/MITP.2017.3680959
[16] Office for Civil Rights, U.S. Department of Health and Human Services. (2013). Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act. Federal Register, 78(17), 5566–5702.
[17] Office for Civil Rights, U.S. Department of Health and Human Services. (2016). HIPAA cloud computing guidance. HHS.gov. https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html

[18] Ponemon Institute. (2023). State of cybersecurity in healthcare 2023. Ponemon Institute LLC. https://www.ponemon.org/research/ponemon-library/security/state-of-cybersecurity-in-healthcare-2023.html
[19] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008
[20] U.S. Congress. (2020). IoT Cybersecurity Improvement Act of 2020, Pub. L. 116-207. https://www.congress.gov/bill/116th-congress/house-bill/1668
[21] Weber, R. H., & Studer, E. (2016). Cybersecurity in the Internet of Things: Legal aspects. Computer Law & Security Review, 32(5), 715–728. https://doi.org/10.1016/j.clsr.2016.07.002
[22] Yousuf, T., Mahmoud, R., Aloul, F., & Zualkernan, I. (2015). Internet of Things (IoT) security: Current status, challenges, and prospective measures. 10th International Conference for Internet Technology and Secured Transactions, 336–341. https://doi.org/10.1109/ICITST.2015.7412116
[23] Zhao, K., & Ge, L. (2013). A survey on the Internet of Things security. 9th International Conference on Computational Intelligence and Security (CIS), 663–667. https://doi.org/10.1109/CIS.2013.145