Building Resilience Security Architecture for Healthcare AI and Robotics: Best Practices

Olusola Gbenga Olufemi
Maryland, USA

Seraphine Agbor
Maryland, USA

ABSTRACT
As healthcare delivery becomes increasingly dependent on AI-driven analytics and robotic systems, ensuring the confidentiality, integrity, and availability of patients' data and automated processes is paramount. This paper surveys the state of the art in security architectures tailored for intelligent and robotic healthcare platforms. It reviews emerging frameworks - Zero Trust, DevSecOps, federated learning, and hardware-rooted trust - and distills best practices in threat modeling, cryptographic data management, network segmentation, and secure development lifecycles. It also illustrates how these approaches interoperate to build layered, resilient defenses against sophisticated cyber-physical threats, compliance gaps, and supply-chain risks. A matrix of frameworks versus capabilities guides practitioners in selecting and integrating security controls that meet both technical and regulatory requirements. Finally, the paper outlines open research challenges and proposes a roadmap for future advances in secure and trustworthy AI and robotics in healthcare.

General Terms
Security architectures; healthcare information systems; AI safety; robotic systems, EHR

Keywords
Resilient Security Architecture; Zero Trust; DevSecOps; Federated Learning; Hardware Security Modules; Clinical Robotics; Data Privacy; Regulatory Compliance

1. INTRODUCTION
The convergence of artificial intelligence (AI) and robotics in healthcare promises transformative advances - from automated diagnostics to minimally invasive robotic surgery - but also expands the attack surface for cyber-physical threats. Modern hospitals and clinics increasingly rely on cloud-based electronic health records (EHRs), AI-driven decision support systems, and network-connected robotic platforms. While these innovations enhance patients 'outcomes and operational efficiency, they introduce new security and privacy risks that traditional perimeter-based defenses and siloed security practices cannot adequately address.

Healthcare organizations must now architect security that:

- **Manages complex data flows** across cloud, edge, and on-premise systems, ensuring that EHRs, medical imaging, and telemedicine streams remain protected in transit and at rest.
- **Protects AI/ML pipelines** from data poisoning, model theft, and adversarial inputs that can undermine diagnostic accuracy and patient safety.
- **Secures robotic platforms** against unauthorized control, firmware manipulation, and supply-chain compromises that could lead to physical harm.
- **Ensures compliance** with stringent regulations, including HIPAA, GDPR, and evolving FDA guidance on AI/ML-driven medical devices.

Research Question. How can healthcare providers build resilient, end-to-end security architectures that integrate best practices and emerging frameworks - such as Zero Trust, DevSecOps, federated learning, and hardware-rooted trust - for AI-driven and robotic systems?

This question can be addressed by:

i. Reviewing foundational and emerging security models (Section 2).

ii. Proposing a layered architecture with core components and controls (Section 3).

iii. Presenting design patterns and case considerations for real-world deployment (Sections 4.1 - 5.4).

iv. Discussing implementation challenges and future research directions (Section 6).

2. RELATED WORK
Early healthcare information technology (IT) security studies emphasized encryption, access controls, and intrusion detection as foundational [4]. More recently, Zero Trust Architectures - where every transaction is authenticated and authorized - have been advocated for protecting EHRs and telehealth platforms [5]. In AI security, federated learning enables collaborative model training without centralizing sensitive patient data, thereby preserving privacy [19]. Adversarial-robust ML methods further defend against input-manipulation attacks [2]. Robotic systems research has focused on real-time safety monitors and secure firmware/OTA update protocols to prevent hijacking and malfunction [1]. While each of these areas has matured independently, a gap persists in consolidated architectures that span the data, model, network, and robotic control layers in healthcare. This framework seeks to bridge this gap.

3. RESILIENT SECURITY ARCHITECTURE FRAMEWORK

3.1 Threat Modeling & Risk Assessment
Robust security architecture begins with systematic threat modeling:

- **Attack Surface Identification:** Enumerate all data sources (EHR, PACS imaging), AI/ML pipelines (training, inference), robot control interfaces (surgical arms, teleoperator links), and hosting environments (cloud, edge nodes).
- **Adversary Profiling:** Consider external threats (ransomware gangs, nation-state actors), internal threats (disgruntled employees), and advanced persistent threats (APTs) targeting intellectual property in AI models.

- **Risk Prioritization:** Apply STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) to each component, ranking risks by their potential impact on patient safety, privacy, and operational continuity.

3.2 Zero Trust Network Segmentation

Zero Trust shifts security enforcement from perimeter defenses to granular, identity-centric controls:

- **Micro-segmentation:** Use software-defined networking to isolate AI analytics clusters, robotic controllers, clinician workstations, and third-party services into distinct security zones.
- **Continuous Authentication:** Employ mutual TLS with device certificates issued by a healthcare PKI, augmented by behavioral biometrics (e.g., typing patterns) to validate both users and robotic endpoints.
- **Monitoring & Analytics:** Leverage IoT-aware SIEM and UEBA (User and Entity Behavior Analytics) to detect anomalous lateral movement, suspicious model queries, and deviations in robotic command sequences.

3.3 Secure Data Management & Privacy

Healthcare data is among the most sensitive; its security is non-negotiable:

- **End-to-End Encryption:** Apply AES-256 encryption at rest and TLS 1.3 in transit. For highly sensitive computations (e.g., genomic analyses), integrate homomorphic encryption to enable operations on encrypted data without decryption.
- **Federated Learning:** Train machine learning models across distributed clinic sites, sharing only encrypted model updates. Combine with differential privacy techniques to add calibrated noise, mitigating patients' re-identification risks.
- **Data Lineage & Provenance:** Record every data access and model-update event on an immutable ledger (e.g., blockchain) to enable forensic auditing, regulatory reporting, and tamper detection.

3.4 DevSecOps & Secure SDLC for AI/Robotics

Incorporate security early and continuously throughout development:

- **Shift-Left Security:** Integrate static application security testing (SAST) and dynamic analysis (DAST) into CI/CD pipelines for both ML code and robotic firmware.
- **Model Assurance:** Enforce adversarial robustness testing (e.g., FGSM, PGD attacks), bias audits, and formal verification of safety-critical decision thresholds.
- **Firmware Integrity:** Employ secure boot and signed OTA updates, managing cryptographic keys within Hardware Security Modules (HSMs) or Trusted Platform Modules (TPMs) embedded in robotic controllers.

4. AUTHORS

Olusola Gbenga Olufemi, PhD, is an information system security leader with a proven track record of securing systems across corporate, healthcare, and academic environments. He uniquely bridges the gap between complex technical execution and rigorous academic research. Armed with advanced certifications, Dr. Olufemi is a dedicated lifelong scholar who also consistently shapes the IT's industry as a technical writer and a peer reviewer.

Dr. Seraphine Agbor, CRNP-PMH, is a board-certified psychiatric nurse practitioner and the CEO of Devoted Wellness & Counseling Services (DWCS) in Maryland, USA. Dr. Agbor is an accomplished healthcare scholar with an enormous wealth of medical expertise.

4.1 A Side-By-Side Comparison of Widely Used Healthcare/Security Frameworks Against Five Capability Areas: Table 1 - 7

Legend: ● = strong/explicit coverage, ○ = partial/indirect, — = not a focus.

Table 1. Framework capability comparison: NIST CSF 2.0 and NIST SP 800-66r2

Framework / standard	Network control	Data privacy	Secure SDLC	Firmware / supply-chain trust	AI/ML model integrity
NIST CSF 2.0 (2024)	● Broad controls across Identify–Protect–Detect–Respond; stronger supply-chain governance in 2.0	○ Privacy risk alignment, not a privacy rule by itself	○ Mentions secure engineering at program level	○ Ties to C-SCRM; governance for third parties	— Focus is general cybersecurity, not AI-specific. (NIST Publications)
NIST SP 800-66r2 (HIPAA guide)	● Implementation guidance for HIPAA controls	● Detailed mapping to HIPAA standards	—	—	—. (NIST Computer Security Resource Center)

Table 2. Framework capability comparison: NIST SSDF and platform firmware resiliency

Framework / standard	Network control	Data privacy	Secure SDLC	Firmware / supply-chain trust	AI/ML model integrity
NIST SP 800-218 (SSDF)	○ High-level requirements may drive secure configs	—	● Secure SDLC practices to reduce vulns	○ Supply-chain references via dependency hygiene	—. (NIST Computer Security Resource Center)
NIST SP 800-193 (Platform Firmware Resiliency)	—	—	—	● Protect-Detect-Recover for platform firmware; supports secure boot & recovery	—. (NIST Computer Security Resource Center)

Table 3. Framework capability comparison: cyber supply-chain risk and AI risk management

Framework / standard	Network control	Data privacy	Secure SDLC	Firmware / supply-chain trust	AI/ML model integrity
NIST SP 800-161 (C-SCRM)	○ Network sourcing/3rd-party risks	○ Privacy via supplier management	○ SDLC supplier expectations	● Comprehensive cyber supply-chain risk guidance	—. (NIST Computer Security Resource Center)
NIST AI RMF 1.0	—	○ Privacy as a trustworthy-AI characteristic	○ SDLC-like AI lifecycle controls	—	● Governance, map/measure/manage AI risks & robustness. (NIST Publications)

Table 4. Framework capability comparison: HIPAA Security Rule and FDA medical-device cybersecurity

Framework / standard	Network control	Data privacy	Secure SDLC	Firmware / supply-chain trust	AI/ML model integrity
HIPAA Security Rule	● TECHNICAL SAFEGUARDS (ACCESS, AUTH, AUDIT)	● EPHI CONFIDENTIALITY/INTEGRITY/AVAILABILITY	— NO PRESCRIPTIVE SDLC	— NOT FIRMWARE/SBOM ORIENTED	— NO AI/ML PROVISIONS. (HHS.GOV)
FDA Cybersecurity in Medical Devices (Premarket) (2025 update)	● Design-time controls; threat modeling; hardening	○ Privacy adjacent but not primary	● Evidence of secure development & maintenance	● SBOMs, secure update/patching, secure boot, TPLC	— (AI aspects handled via separate GMLP). (U.S. Food and Drug Administration)

Table 5. Framework capability comparison: HITRUST CSF and HHS 405(d) HICP

Framework / standard	Network control	Data privacy	Secure SDLC	Firmware / supply-chain trust	AI/ML model integrity
HITRUST CSF	● DETAILED, CERTIFIABLE CONTROL SET INCL. NETWORK	● INTEGRATES PRIVACY MAPPINGS	● DEVELOPMENT & CHANGE-CONTROL REQUIREMENTS	○ VENDOR RISK & SOME SBOM/SCRM EXPECTATIONS	— (NOT AI-SPECIFIC). (HITRUST ALLIANCE)
HHS 405(d) HICP	● Emphasizes inventorying devices & segmentation for HDOs	○ Privacy via safeguards, not a privacy standard	—	○ Device/security hardening practices	—. (405d.hhs.gov)

Table 6. Framework capability comparison: IEC health-network and medical-software standards

Framework / standard	Network control	Data privacy	Secure SDLC	Firmware / supply-chain trust	AI/ML model integrity
IEC 80001-1:2021	● RISK MGMT FOR HEALTH IT NETWORKS W/ MEDICAL DEVICES	○ ADDRESSES "KEY PROPERTIES" INCL. SECURITY (AND IMPLICITLY PRIVACY)	—	○ RISK APPROACH TOUCHES CONNECTED DEVICE TRUST	—. (ISO)
IEC 62304 (medical software lifecycle)	—	—	● Medical-grade software lifecycle & change control	○ Post-market maintenance intersects with update trust	—. (ISO)

Table 7. Framework capability comparison: privacy management and good machine-learning practice

Framework / standard	Network control	Data privacy	Secure SDLC	Firmware / supply-chain trust	AI/ML model integrity
ISO/IEC 27701 (PIMS)	—	● PRIVACY INFORMATION MANAGEMENT SYSTEM (PIMS)	—	—	—. (ISO)
GMLP (FDA/IMDRF)	—	○ User transparency & human-AI teaming principles	○ ML-specific dev/validation best practices	—	● Principles for safe/effective ML in medical devices; transparency & change control. (U.S. Food and Drug Administration)

- HIPAA Security Rule modernization proposal (Jan - Mar 2025 comment period) adds segmentation/ - specifics applicable if you're planning upgrades soon. (Reuters)
- FDA's 2025 premarket update supersedes 2023 and reinforces SBOM + lifecycle security - helpful for device vendors & HDO procurement. (RAPS)

Now is the moment to adapt the comparison discussed in the tables above into a **controls-to-frameworks RACI/requirements checklist** specifically for Devoted Wellness & Counseling Services (DWCS). As a healthcare provider handling sensitive patients' data, DWCS prioritizes HIPAA compliance, secure workflows, and the safe adoption of technology. Below is a tailored view of the adoption:

DWCS Controls-to-Frameworks RACI/Requirements Checklist

Legend

- **R** = Responsible (control implementers, e.g., IT/security staff, developers)
- **A** = Accountable (executive/leadership sign-off, e.g., CIO/Compliance Officer)
- **C** = Consulted (legal, clinicians, external vendors)
- **I** = Informed (all staff, patients, stakeholders)

A. Network Control

Control	Framework References	RACI at DWCS
Segmentation of clinical vs admin networks	HIPAA Security Rule §164.312, HICP, NIST CSF	R: IT staff; A: Compliance Officer; C: Clinical Operations; I: All staff
Zero-Trust access & MFA	NIST CSF, HITRUST, HICP	R: IT staff; A: CIO; C: Vendor (EHR/cloud); I: Users
Continuous monitoring & logging	NIST CSF, HITRUST	R: IT staff; A: Security Lead; C: Compliance Officer; I: Leadership

B. Data Privacy

Control	Framework References	RACI at DWCS
ePHI governance & consent	HIPAA Privacy & Security Rules, ISO 27701	R: Compliance team; A: Privacy Officer; C: Legal counsel; I: Patients
Encryption (in transit & at rest)	HIPAA, HITRUST, NIST CSF	R: IT/security staff; A: CIO; C: Cloud vendor; I: Staff

Control	Framework References	RACI at DWCS
Data minimization & retention policies	HIPAA, NIST SP 800-66, ISO 27701	R: Compliance team; A: Privacy Officer; C: Clinical staff; I: Patients

C. Code Quality & Secure Development

Control	Framework References	RACI at DWCS
Secure SDLC & vulnerability scanning	NIST SP 800-218 SSDF, IEC 62304 (if medical software developed)	R: Developers/contractors; A: CTO or CIO; C: QA/Compliance; I: Leadership
Patch management process	NIST CSF, FDA Cybersecurity Guidance	R: IT staff; A: Security Lead; C: Vendor; I: End-users
Secure configuration baselines	HITRUST, NIST CSF	R: IT staff; A: Security Lead; C: Cloud vendor; I: Staff

D. Firmware Trust & Supply Chain

Control	Framework References	RACI at DWCS
Vendor device assurance (SBOM, secure boot)	FDA Premarket Cybersecurity Guidance (2025), NIST SP 800-193, NIST SP 800-161	R: Procurement/IT; A: CIO; C: Device vendor, Clinical Engineering; I: Compliance team
Medical device lifecycle monitoring	IEC 80001, HICP	R: IT/Clinical Engineering; A: Compliance Officer; C: Clinicians; I: Leadership
Supplier risk assessments	NIST SP 800-161 C-SCRM, HITRUST	R: Procurement; A: Compliance Officer; C: Vendors; I: Leadership

E. Model Integrity (AI/ML in Care or Admin Tools)

Control	Framework References	RACI at DWCS
AI model validation & bias testing	NIST AI RMF, FDA GMLP	R: Data science/AI vendor; A: CIO/Clinical Lead; C: Compliance, Clinical staff; I: Patients
Transparency & explainability to clinicians	NIST AI RMF, GMLP	R: AI vendor; A: Clinical leadership; C: Compliance Officer; I: Clinicians
Monitoring for drift & performance	NIST AI RMF, HITRUST	R: IT/AI staff; A: CIO; C: Vendor, Clinical staff; I: Leadership

Table A–E highlights how this adoption provides substantial support to DWCS. It helps to:

- Create a **checklist** that leadership can use to track for compliance.
- Assign **clear accountability** for each control area.
- Align DWCS practices with **healthcare-specific frameworks** (HIPAA, FDA, HICP) while extending into **newer domains** (firmware trust, AI/ML governance).

I. Best-Practices Checklist for Healthcare AI and Robotics Security

Practice	Description
Threat Modeling Review	Annual STRIDE assessment for data, models, and devices.
PKI & Certificate Rotation	Rotate TLS and device certificates every 90 days; revoke compromised credentials immediately.
Federated Learning Audits	Verify client data distributions and inspect gradient updates for potential poisoning attempts.
Continuous Red-Team Testing	Simulate adversarial ML and robotic intrusion scenarios quarterly.
Compliance Automation	Embed HIPAA/GDPR checks into CI/CD; generate immutable audit logs on each deployment.

II. Regulatory Integration and Governance

- **Policy Frameworks:** Map each control to relevant regulations - HIPAA Security Rule, GDPR Article 32, FDA guidance on AI/ML SaMD - ensuring no compliance gaps.
- **Governance Structures: Form a cross-functional Security & AI Ethics board comprising CISOs, clinical engineers, data scientists, and legal advisors to review risk-acceptance decisions and oversee incident response**

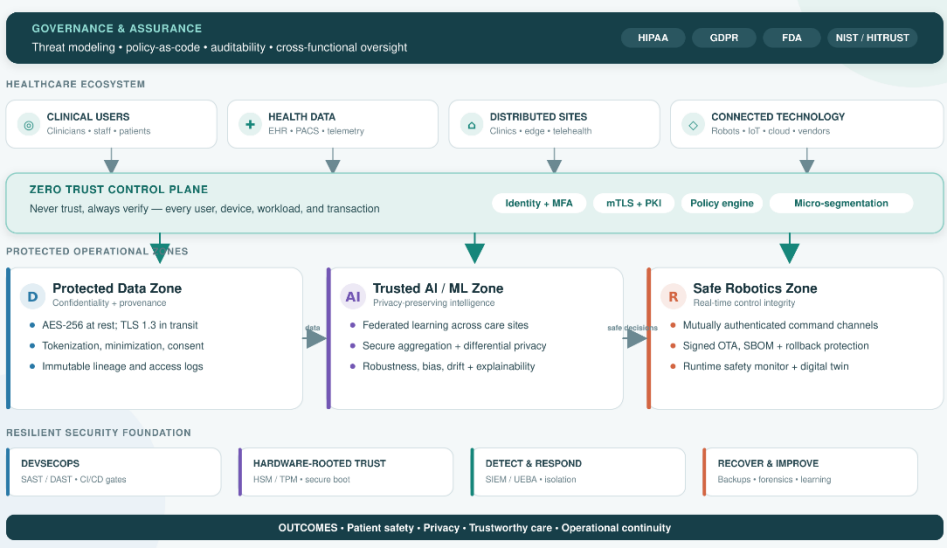

Fig: 1: Layered Control Preserves Patients' Safety, Privacy, Clinical Continuity

5. DESIGN PATTERNS AND DEPLOYMENT CONSIDERATIONS

The deployment of resilient, secure architectures for AI-driven and robotic healthcare systems requires careful orchestration of multiple control layers - from cloud-based infrastructure to endpoint robotic devices. These layers must interoperate seamlessly without compromising performance, compliance, or patient safety [36];[9]. This section presents design patterns and implementation scenarios drawn from both literature and real-world healthcare environments.

5.1 Layered Defense Pattern (Defense-in-Depth)

A multi-layered approach ensures that a single failure does not compromise the system. Each tier - **data**, **application**, **network**, and **device -** implements overlapping safeguards. See Fig. 1, which outcomes result in patient safety, trusted care, privacy and operational continuity.

- **Data Layer:** Employ encryption, tokenization, and differential privacy [11].
- **Application Layer:** Integrate runtime application self-protection (RASP) and AI model monitoring for anomaly detection [12;13].
- **Network Layer:** Apply Zero Trust micro-segmentation and continuous identity verification [5].
- **Device Layer:** Enforce hardware-based attestation using TPM or HSM modules to ensure firmware trust [16;17].

Each layer also aligns with compliance mandates such as the HIPAA Security Rule and NIST Cybersecurity Framework (CSF) functions - **Identify**, **Protect**, **Detect**, **Respond**, and **Recover** [8;10].

5.2 Federated and Privacy-Preserving AI Pattern

For distributed healthcare systems like the one in **DWCS,** where clinics may operate across multiple sites, **federated learning** offers a secure alternative to centralizing patient data.

- Each clinic trains local models and shares encrypted model updates, aggregated through a secure coordination server [19].
- Differential privacy ensures that shared gradients do not leak identifiable patient information [11].
- Someone can use homomorphic encryption or secure multi-party computation (SMPC) to ensure that aggregation operations are performed on encrypted data [14;15].

This pattern supports regulatory compliance (HIPAA, GDPR) while improving model accuracy and cross-site collaboration.

5.3 Robotic Security Integration Pattern

Clinical robotics - used in tele-surgery, medication dispensing, or rehabilitation - requires both real-time control integrity and safe autonomy [1;20].

- Implement secure command channels with mutual authentication and signed control messages.
- Deploy runtime safety monitors that halt robotic movement upon detection of anomalous sensor data or command sequences [21].
- Incorporate over-the-air (OTA) update frameworks signed with asymmetric keys to ensure firmware authenticity and prevent rollback attacks [38].
- Maintain digital twins of robotic platforms for testing updates before production deployment [39].

5.4 Compliance and Audit Automation Pattern

Automated compliance management supports continuous assurance and governance across healthcare IT ecosystems [28].

- Implement policy-as-code solutions that encode HIPAA, GDPR, and FDA requirements into automated audit scripts [27].
- Generate continuous compliance reports for internal auditors and regulators via integrated SIEM dashboards.

- Use immutable audit trails (blockchain-backed) to demonstrate traceability and non-repudiation [24].

6. IMPLEMENTATION CHALLENGES AND FUTURE RESEARCH ROADMAPS

Despite notable progress, the secure deployment of AI and robotic systems in healthcare remain challenging - these span technical, regulatory, and organizational domains.

6.1 Key Implementation Challenges

6.1.1 Legacy Integration and Interoperability

Many healthcare institutions continue to operate legacy EHR systems and outdated device firmware that were never designed for Zero Trust or federated architectures [4]. Integrating these with modern AI platforms introduces compatibility and latency issues. Research is needed on secure middleware and interoperability standards that bridge older HL7/FHIR systems with modern security layers [25].

6.1.2 AI Model Meaning and Validation

While adversarial robustness and fairness testing have improved, the meaning of AI-driven clinical decisions remains a regulatory and ethical concern [26]. Lack of interpretability may hinder FDA clearance or clinician adoption. Emerging techniques such as SHAP and LIME offer partial visibility but require formal standardization for medical-grade use.

6.1.3 Supply-Chain and Firmware Trust

Healthcare robotics and IoT ecosystems rely heavily on third-party hardware vendors. Vulnerabilities introduced at the manufacturing or firmware level can compromise the entire trust chain [23]. Implementing continuous SBOM (Software Bill of Materials) verification and vendor attestation is still nascent and requires broader regulatory enforcement [9].

6.1.4 Continuous Compliance Under Evolving Regulations

As regulators (FDA, HHS, EU AI Act) update standards for AI-driven healthcare, compliance frameworks must evolve dynamically. Organizations like DWCS must adopt adaptive governance systems capable of real-time updates to policies and controls [22];[29].

6.2 Roadmap for Future Research

6.2.1 Autonomous Threat Intelligence and Self-Healing Systems

Next-generation healthcare networks will leverage AI-driven threat intelligence to detect, predict, and autonomously mitigate cyberattacks [13]. Integrating self-healing architectures - where compromised components automatically isolate and restore themselves - remains an open research area [30].

6.2.2 Explainable and Auditable AI for Clinical Decision Support

Research should prioritize auditable AI frameworks that enable regulators to trace training data lineage, access fairness metrics, and review decision logs. Integration with blockchain or secure provenance systems can enhance transparency [4];[26].

6.2.3 Quantum-Resistant Cryptography for Healthcare Data

As quantum computing advances, current cryptographic standards (e.g., RSA, ECC) are becoming obselete. Future healthcare architectures must integrate **post-quantum cryptography (PQC)** and hybrid encryption to safeguard long-term patient data [32];[33].

6.2.4 Human-Centered Security and Organizational Culture

Even the most advanced security frameworks fail without user adherence. Building a security-aware culture - through continuous training, behavioral analytics, and incentive-driven compliance - remains a top priority [34];[10].

6.3 Concluding Remarks

Securing AI and robotic systems in healthcare demands a holistic fusion of technical innovation, regulatory compliance, and human-centered governance. By integrating Zero Trust, DevSecOps, federated learning, and hardware-rooted trust within a layered, adaptive architecture, healthcare organizations like DWCS can achieve both resilience and trustworthiness. The next frontier lies in developing self-defending, explainable, and compliant ecosystems - where patient safety, privacy, and care quality remain the core metrics of success.

7. ACKNOWLEDGMENTS

The authors express their sincere appreciation to the leadership and staff of DWCS, Maryland, for their invaluable insights into the challenges and opportunities of technology adoption in healthcare environments. Special thanks are extended to the information security professionals and healthcare practitioners who shared their perspectives on secure architecture design, data governance, and AI and robotic system safety. Authors also acknowledge the guidance of open standards bodies - including the National Institute of Standards and Technology (NIST), the U.S. Food and Drug Administration (FDA), and the Health Information Trust Alliance (HITRUST) - whose frameworks informed the architectural models and control mappings presented in this study. Finally, gratitude is due to the research and engineering communities whose foundational work in Zero Trust Architecture, DevSecOps, Federated Learning, and Hardware-Based Security shaped the direction of these resilient, AI-driven healthcare innovations.

8. REFERENCES

[1] Alami, R., et al. (2016). Safe human-robot interaction in surgical environments. IEEE Trans. Medical Robotics & Bionics, 2(1), 45–56.

[2] Goodfellow, I., Shlens, J., & Szegedy, C. (2015). Explaining and Harnessing Adversarial Examples. *ICLR*.

[3] Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated Learning: Challenges, Methods, and Future Directions. IEEE Signal Processing Magazine, 37(3), 50–60.

[4] Raghupathi, W., & Raghupathi, V. (2014). Big Data Analytics in Healthcare: Promise and Potential. Health Information Science and Systems, 2(1), 3.

[5] Rose, S., et al. (2020). Zero Trust Architecture. NIST SP 800-207.

[6] Tufte, E. R. (2001). The Visual Display of Quantitative Information. Graphics Press.

[7] Venable, H., et al. (2018). DevSecOps for Medical Device Software: A Methodology. Journal of Medical Systems, 42(12), 250.

[8] NIST, 2024, The NIST Cybersecurity Framework (CSF) 2.0, https://doi.org/10.6028/NIST.CSWP.29,

[9] FDA, 2023, 2023 Device Approvals, https://www.fda.gov/medical-devices/recently-approved-devices/2023-device-approvals

[10] HHS, 2022, HHS Fiscal Year 2022 Freedom of Information Annual Report, https://www.hhs.gov/foia/reports/annual-reports/2022/index.html,

[11] Dwork & Roth, 2014, The Algorithmic Foundations of Differential Privacy. Foundations and Trends in Theoretical Computer Science 9, 3–4 (2014), 211–407. https://doi.org/10.1561/0400000042

[12] Papernot et al., 2016, The Limitations of Deep Learning in Adversarial Settings,

[13] Gartner, 2023, Gartner, Market Guide for Digital Experience Monitoring, 20 November 2023

[14] Gentry, 2009, Gentry, C. (2009) Fully Homomorphic Encryption Using Ideal Lattices. ACM Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, 31 May-2 June 2009, 169-178

[15] Bonawitz et al., 2019, Towards Federated Learning at Scale: System Design, February 2019, DOI:10.48550/arXiv.1902.01046

[16] NIST SP 800-193, 2018, Platform Firmware Resiliency Guidelines, https://doi.org/10.6028/NIST.SP.800-193

[17] Dolev et al., 2019, ommunication complexity of byzantine agreement, revisited. In ACM Symposium

[18] on Principles of Distributed Computing (PODC), pages 317–326, 2019

[19] Li et al., 2020, 'Knowledge structure of technology licensing based on co-keywords network, DOI:10.1016/j.iref.2021.03.018

[20] Zhang et al., 2021, Coporate environmenta information disclosure and stock price crash risk: Evidence from Chinese listed heavily polluting companies, Elsevier, DOI:10.2139/ssrn.3906505

[21] Chen et al., 2023, Digital transformation and firm performance: a case study on China's listed companies 2009-2020, https://doi.org/10.1007/s44265-023-00018-x

[22] HITRUST, 2023, HITRUST Collaborate 2023: Being Informed and Aware in Cybersecurity, Gaylord Texan Resort and Convention Center, Grapevine, TX

[23] NIST SP 800-218, 2022, Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities, https://doi.org/10.6028/NIST.SP.800-218

[24] Casino et al., 2019, A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues. Telematics and Informatics, 36, 55-81, https://doi.org/10.1016/j.tele.2018.11.006

[25] HL7, 2022, HL7 36th Annual Plenary & Working Group Meeting (WGM) held in Baltimore, MD

[26] Ribeiro et al., 2016, "Why Should I Trust You?" Explaining the Predictions of Any Classifier, https://doi.org/10.1145/2939672.2939778

[27] NIST SP 800-161r1, 2022, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, https://doi.org/10.6028/NIST.SP.800-161r1-upd1

[28] HITRUST, 2023, HAA 2023-010: HITRUST Risk Management Handbook

[29] European Commission, 2024, The EU in 2024, General Report on the Activities of the European Union

[30] Kandias et al., 2010, An insider threat prediction model. In: Katsikas, S., Soriano, M., Lopez, J. (eds.) International Conference on Trust, Privacy and Security in Digital Business, pp. 26–37. Springer,

[31] Casino et al., 2019, A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues. Telematics and Informatics, 36, 55-81, https://doi.org/10.1016/j.tele.2018.11.006

[32] Chen et al., 2016, Untangling the Relatedness among Correlations, Part II, https://afni.nimh.nih.gov/pub/dist/doc/htmldoc/codex/fmri/2016_ChenEtal.html

[33] NIST PQC, 2023, Quantum-Readiness: Migration from Post-Quantum Cryptography, https://www.cisa.gov/sites/default/files/2023-08/Quantum%20Readiness_Final_CLEAR_508c%20%283%29.pdf

[34] Killourhy & Maxion, 2009, Comparing anomaly-detection algorithms for keystroke dynamicsDOI:10.1109/DSN.2009.5270346

[35] HHS, 2022, HHS Fiscal Year 2022 Freedom of Information Annual Report https://www.hhs.gov/foia/reports/annual-reports/2022/index.html

[36] NIST, 2024, Safeguarding Health Information: Building Assurance through HIPAA Security 2024, Washington, DC

[37] Zheng, Z., & Xie, S. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. Proc. IEEE BigData.

[38] Chaudhry & Shin, 2022, Artificial intelligence in Education (AIEd): a high-level academic and industry note 2021. AI and Ethics . 2022;2(1):157–165. doi: 10.1007/s43681-021-00074-z

[39] Lee et al., 2020, Application of Artificial Intelligence-Based Technologies in the Healthcare Industry: Opportunities and Challenge.