GAS Journal of Engineering and Technology (GASJET)

Volume 3 | Issue 9, 2026 Homepage: https://gaspublishers.com/gasjet-home/ ISSN: 3048-5800

Integrating Cybersecurity Controls across IT/OT Environments in the Medical Sector- A Review of Threats, Standards and an Integrated Control Framework for Healthcare Information Technology and Operational Technology

Peter Wonah Odey; Membu Judy Chude; Nwagbara Chisom Telvin

Emails: Odeypeter@nsuk.edu.ng; jcmembu@yahoo.com; telvinchisom@gmail.com

Department of Cyber Security, Center for Cyberspace Studies, Nasarawa State University Keffi, (NSUK), Nassarawa State, Nigeria

Received: *20.08.2026* | ***Accepted:*** *03.09.2026* | ***Published:*** *18.09.2026*

***Corresponding Author** Membu Judy Chude

DOI: *10.5281/zenodo.22828833*

Abstract **Review Article**

Modern healthcare depends on a dense network of digital systems, connected medical devices and operational technologies. Electronic health records, imaging systems, infusion pumps, patient monitors, cloud platforms and building-control systems now exchange data continuously. This connectivity improves clinical work, but it also creates routes through which a weakness in one system can affect many others. The problem is not simply a shortage of security tools. In many organisations, information technology, clinical engineering, procurement and operational teams manage risk separately, while suppliers retain significant control over device updates and remote access. This review examines recent evidence on medical-device vulnerabilities, healthcare supply-chain exposure, procurement practice and governance across converged IT/OT environments. It finds that known weaknesses remain common in connected devices; cybersecurity conditions are still absent from many tender and contract documents; and fragmented accountability allows local weaknesses to become organisation-wide risks. In response, the paper proposes a four-layer control framework built around shared asset visibility, consistent risk assessment, unified governance and resilient care delivery supported by continuous monitoring. The framework draws on the NIST Cybersecurity Framework, NIST Zero Trust guidance, ISO/IEC 27001, IEC 62443 and medical-device safety requirements. For Nigerian healthcare organisations, the approach is intended to be practical: begin with accurate inventories, protect high-risk clinical systems, place measurable security obligations in procurement documents, and strengthen coordination between IT, clinical engineering, management and vendors.

Keywords: IT/OT convergence; healthcare cybersecurity; Internet of Medical Things; medical-device security; cybersecurity governance; Nigeria.

1. Introduction

Healthcare is now as dependent on reliable digital infrastructure as it is on trained clinicians. Hospital information systems, electronic health records, diagnostic equipment, infusion pumps, patient monitors, telemedicine platforms and wearable

sensors form a connected environment usually described as the Internet of Medical Things (IoMT). In larger hospitals, the number of networked devices may exceed the number of beds many times over (Akram et al., 2026; Filani et al., 2026). These systems improve access to information, support remote monitoring and reduce delays in clinical decision-making. They also mean that a cyber incident can disrupt both information and patient care.

Information technology (IT) covers data, applications, servers and communication systems. Operational technology (OT) refers to systems and devices that monitor or control physical processes. In healthcare, OT includes medical imaging equipment, infusion pumps, laboratory automation, building-management systems, power controls and other devices that directly support clinical work. The boundary between these two domains is steadily disappearing. Clinical devices send information to hospital systems, vendors connect remotely for maintenance, and cloud platforms receive data from both IT and OT networks.

This convergence brings clear benefits, but it also gives attackers more ways to move through an organisation. A stolen password, an insecure vendor connection or an unpatched device may become the starting point for a wider incident. The consequences can include loss of confidential records, cancelled appointments, delayed diagnosis, interruption of treatment and risk to patient safety. The financial impact is also substantial. IBM (2025) reported that healthcare remained the industry with the highest average cost per data breach, while the time required to identify and contain incidents remained lengthy.

This paper reviews the main risks at the healthcare IT-OT boundary, considers the standards available to manage those risks, and proposes an integrated framework that brings technical security, procurement and governance into one coherent approach.

2. IT/OT Convergence in Healthcare: Concepts and Drivers

IT and OT developed with different priorities. Traditional IT security focuses on protecting the confidentiality, integrity and availability of information. OT teams place particular emphasis on safety, reliability and uninterrupted operation. These priorities overlap in hospitals, but they are not always identical. A software update that is routine on an office computer may be unsafe on a certified medical device if it interrupts treatment or invalidates the manufacturer's approval.

Convergence occurs because modern care requires information to move between clinical devices and business systems. Telehealth extends care beyond hospital walls. Remote patient monitoring sends data over public or mobile networks. Cloud-based hospital systems receive information from devices on wards and in patients' homes. This makes shared visibility essential. Security teams cannot protect equipment they do not know exists, and clinical teams cannot make informed decisions if they do not understand the security condition of the systems on which they rely (İmamoğlu, 2025).

The aim should not be to force IT and OT into a single technical environment. It should be to manage them through a common view of assets, identities, risks and responsibilities. That approach allows each domain to retain its operational requirements while reducing the gaps between them.

3. Threat Landscape at the Healthcare IT/OT Boundary

The most persistent threats at the IT/OT boundary are ransomware, phishing, stolen credentials, insider mistakes, insecure medical devices and third-party compromise. Artificial intelligence may help attackers prepare more convincing messages or automate reconnaissance, but the underlying weaknesses remain familiar: weak authentication, poor network separation, outdated software and insufficient monitoring.

Ransomware is especially damaging because hospitals cannot easily suspend services while an investigation takes place. Current campaigns often combine encryption with data theft and pressure on suppliers or patients. A breach at one service provider may affect billing, pharmacy systems, claims processing and patient access across several

healthcare organisations (Filani et al., 2026).

Connected medical devices are attractive entry points because many were designed primarily for clinical reliability rather than modern cybersecurity. A review of 150 IoMT devices reported known vulnerabilities in 74 per cent of sampled infusion pumps, 72 per cent of imaging systems, 70 per cent of hospital information systems, 63 per cent of patient monitors and 47 per cent of wearable devices (Akram et al., 2026). Although the percentages differ by category, the broader message is straightforward: vulnerability is widespread rather than exceptional.

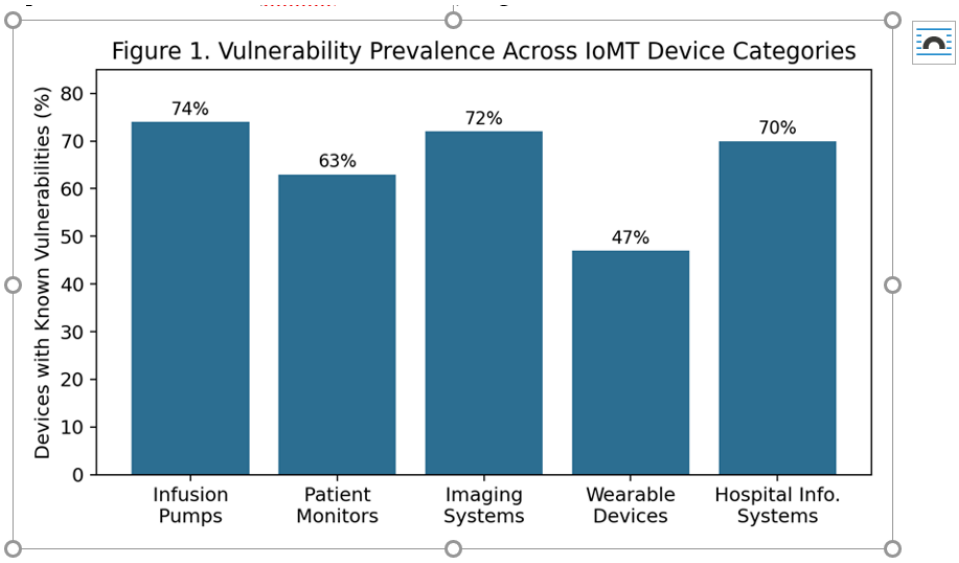

Figure 1. Percentage of sampled devices with known vulnerabilities by IoMT category. Adapted from Akram et al. (2026).

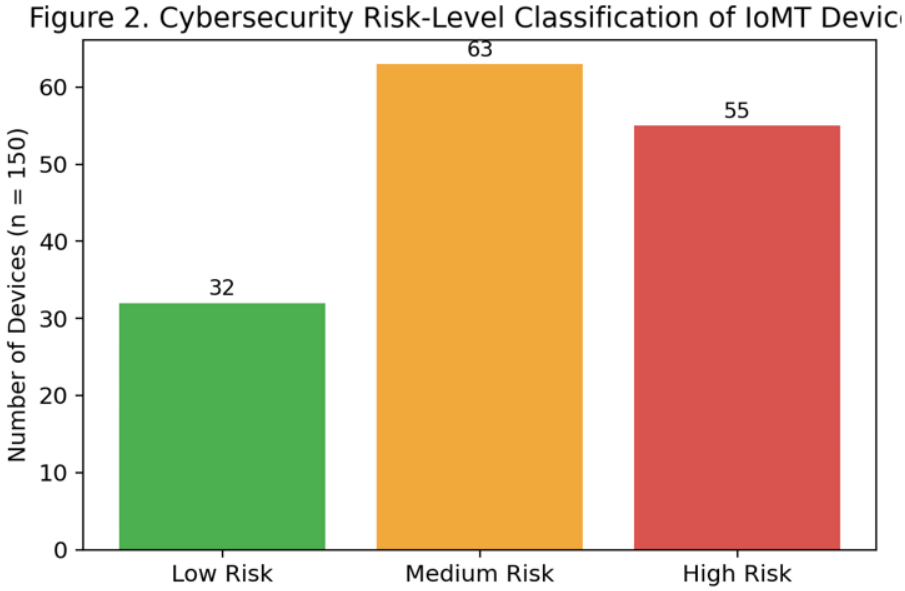

Figure 2. Overall risk classification of 150 sampled IoMT devices. Adapted from Akram et al. (2026).

3.1 Recurring Technical Weaknesses

Technical security advisories often use Common Weakness Enumeration (CWE) codes. These codes are useful to specialists, but they are not self-explanatory to managers, procurement officers or clinical staff. Table 1 therefore presents the same weaknesses in plain UK English. The advisory count shows how often each weakness appeared in the reviewed security notices; it does not mean that every device contains the weakness.

Technical reference	Plain-English meaning	What it means in practice	Advisories
CWE-287	Identity is not checked properly	The system may allow the wrong person or device to log in or gain access.	59
CWE-798	A fixed password or key is built into the product	Attackers may use a known default credential that users cannot easily change.	46
CWE-330	Security values are too predictable	Passwords, tokens or encryption values may be guessed more easily than they should be.	41
CWE-20	Unsafe or unexpected input is accepted	The system does not properly check data before processing it.	34
CWE-522	Passwords or security keys are not adequately protected	Credentials may be stored or sent in a way that exposes them to attackers.	31
CWE-120	Too much data can be copied into a limited memory area	A software error may allow a crash or unauthorised code to run.	29
CWE-79	Website input is not safely handled	An attacker may insert harmful browser code, commonly called cross-site scripting.	27
CWE-319	Sensitive information is sent without encryption	Anyone able to intercept the connection may read the information.	26
CWE-306	A critical function can be used without logging in	Sensitive actions may be available without proper authentication.	21

Table 1. Common medical-device software weaknesses explained for non-technical readers. CWE means Common Weakness Enumeration.

3.2 Supply-Chain and Vendor-Dependent Risk

Healthcare organisations rely heavily on billing companies, cloud providers, imaging partners, maintenance contractors and medical-device manufacturers. These relationships create shared risk because one compromised supplier may provide

access to several customers. The risk is increased when hospitals are not permitted to patch or reconfigure equipment without vendor approval. In such cases, a known weakness may remain in service for years because the clinical and contractual consequences of changing the device are considered too high (Akram et al., 2026; Filani et al., 2026).

ENISA (2023) found that ransomware accounted for 54 per cent of reported cyber incidents in the European health sector between January 2021 and March 2023. Incidents affecting suppliers or service partners also caused disruption to downstream organisations. Information-sharing bodies such as Health-ISAC can help providers that do not have large internal threat-intelligence teams, but information sharing is most useful when organisations have the staff and processes required to act on it.

4. Governance Fragmentation and Procurement Gaps

Technical controls cannot compensate for unclear accountability. Mengnjo (2026) assessed six units within one large healthcare system and found meaningful differences in security monitoring, participation in assessment activities and overall preparedness. The important point is not that every unit must have identical technology. It is that one poorly governed unit can expose better-managed units when they share data, suppliers or infrastructure.

Procurement evidence shows a similar weakness. Pandey and Kumar (2026) analysed 760 public-hospital procurement documents and compared the language with medical-device security advisories. Only 15 per cent of the documents contained cybersecurity-related terms. By contrast, routine operational terms such as warranty, equipment and maintenance appeared in most tenders. Even where security was mentioned, the wording was often broad and difficult to enforce. A tender may ask for 'security' or 'antivirus' without specifying encryption, authentication, patching periods or incident-reporting duties.

These studies point to the same conclusion from different directions: cybersecurity is still treated as a specialist concern rather than a condition of purchasing, operating and governing medical technology.

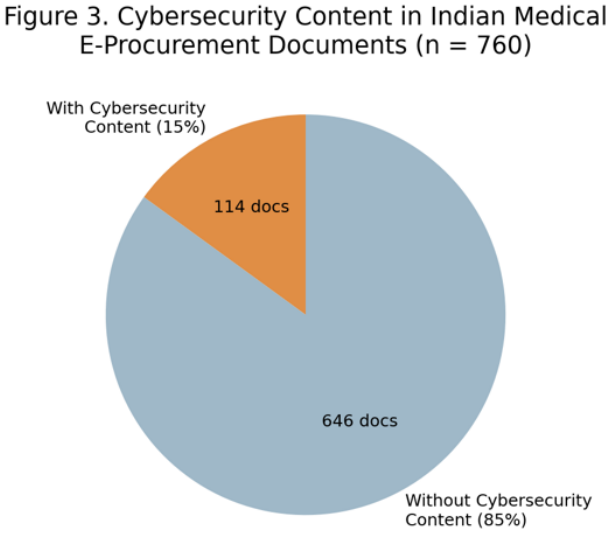

Figure 3. Cybersecurity content in 760 medical e-procurement documents. Adapted from Pandey and Kumar (2026).

Study	Method in plain English	Evidence examined	Main finding
Mengnjo (2026)	The same cybersecurity self-assessment was applied to several departments so that results could be compared fairly.	Six supply-chain-related units in one large healthcare system.	Security maturity differed substantially. Weak coordination and dependence between units increased organisation-wide risk.
Pandey and Kumar (2026)	Computer-assisted text analysis was used to identify words and themes in tender documents and compare them with security advisories.	760 medical e-procurement documents issued between 2014 and 2024.	Only 15% of tenders referred to cybersecurity. ISO/IEC 27001-family standards appeared in fewer than 2% of the reviewed documents.

Table 2. Comparison of governance-gap findings in two empirical healthcare cybersecurity studies.

5. Standards and Regulatory Landscape

No single standard covers every part of a converged healthcare environment. The practical task is therefore to use complementary standards without turning them into separate compliance exercises. Table 3 explains the main frameworks in plain language and shows how each contributes to an integrated approach.

The NIST Cybersecurity Framework 2.0 provides an organisation-wide structure based on Govern, Identify, Protect, Detect, Respond and Recover (NIST, 2024). NIST SP 800-207 provides the basis for Zero Trust, under which users, devices and services are continuously verified rather than trusted because of their location (NIST, 2020). ISO/IEC 27001 and 27002 support information-security governance and control selection. IEC 62443 offers a particularly useful model for OT because it separates systems into security zones and controls the connections between them. Medical-device standards such as ISO 13485 and ISO 14971 support product quality and safety, but they do not replace information-security controls.

For Nigeria, these international frameworks should be applied alongside the Nigeria Data Protection Act, sectoral health obligations and public-procurement requirements. International standards offer recognised methods; Nigerian law and institutional policy determine how those methods are governed and enforced locally.

Framework or standard	Area covered	Plain-language purpose	Use for converged healthcare
FDA Premarket Cybersecurity Guidance	Medical-device design and manufacture	Requires manufacturers to consider cyber threats, updates and a software bill of materials before a device is marketed.	Strong for product design, but its value depends on hospitals carrying the requirements into procurement and contracts.
NIST Cybersecurity Framework 2.0	Organisation-wide IT and OT risk	Provides six activities: govern, identify, protect, detect, respond	A useful overall structure, although adoption is

Framework or standard	Area covered	Plain-language purpose	Use for converged healthcare
	management	and recover.	voluntary and may vary by provider.
HHS 405(d) Health Industry Cybersecurity Practices	Healthcare organisations	Provides practical security measures scaled to the size and resources of a healthcare provider.	Useful alongside the NIST framework, especially for common healthcare threats.
NIST SP 800-207 Zero Trust	Identity and access	Requires continual verification of users, devices and services rather than trusting them because they are inside the network.	Supports controlled access across segmented clinical networks.
ISA/IEC 62443	Operational technology and industrial control systems	Separates systems into security zones and controls the connections between them.	Highly relevant to medical devices and hospital operational systems.
ISO/IEC 27001 and 27002	Information-security governance and controls	Creates an auditable management system for selecting, operating and improving security controls.	Strong governance baseline, but often weakly represented in medical-device procurement.

Table 3. Main security frameworks and standards explained in plain UK English.

6. An Integrated IT/OT Cybersecurity Control Framework

The proposed framework contains four connected layers. It is deliberately simple so that senior managers, clinicians, engineers, procurement officers and security specialists can use the same model.

1. Shared asset and data visibility. The organisation maintains one reliable inventory of IT systems, OT equipment, IoMT devices, software, users, data flows, suppliers and remote connections. Each asset has an owner, a location, a support status and a clear record of the information or service it handles. Network zones and controlled connections limit the movement of an attacker from one area to another.

2. Integrated risk and threat assessment. IT and OT assets are assessed using the same broad criteria, while allowing for differences in patient-safety impact. A useful risk score considers how likely a threat is, how serious the weakness is and what would happen if the asset failed or were compromised. In plain language: risk rises when an attack is more likely, the weakness is more serious, or the clinical and operational consequences are greater. The formula is a decision aid, not a substitute for professional judgement.

3. Governance, policy and compliance. One cross-functional body oversees cybersecurity across IT, clinical engineering, OT, procurement, legal services and senior management. This body maps the relevant standards and laws to a single control set, approves risk exceptions and ensures that suppliers meet contractual obligations. The purpose is to avoid three

separate compliance silos for IT, medical devices and operational systems.

4. Resilient and patient-safe care delivery. Monitoring, incident response, backup, recovery and business-continuity arrangements are designed around clinical priorities. Analytics can help identify unusual network behaviour, device activity or user access, but automated alerts must be reviewed by competent staff. Security action should reduce risk without creating avoidable harm to patients.

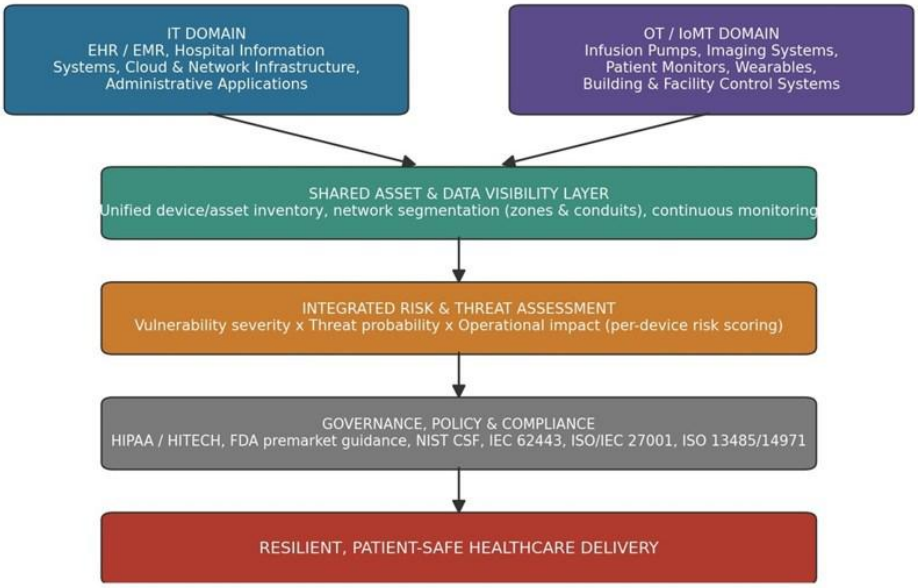

Figure 4. Four-layer integrated cybersecurity control framework for healthcare IT and OT.

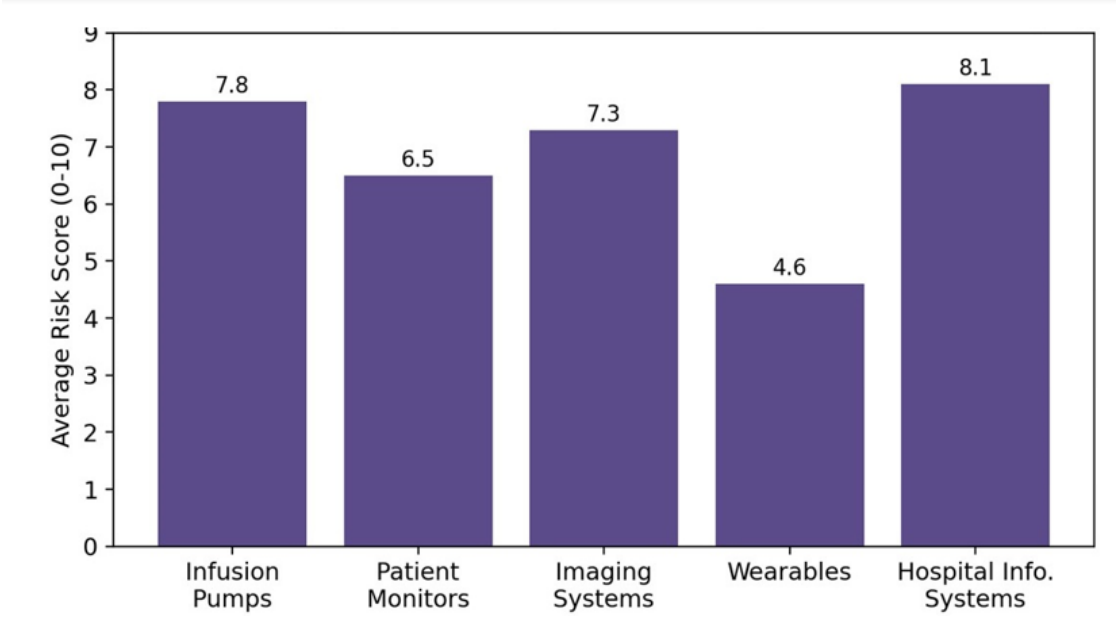

Figure 5. Average cybersecurity risk score by IoMT device category. Adapted from Akram et al. (2026).

7. Embedding Security in Procurement and Vendor Management

Procurement is one of the most effective places to improve security because requirements can be agreed before a device enters the network. General phrases such as 'the system must be secure' are too vague. Contracts should set measurable expectations for authentication, encryption, software updates, vulnerability disclosure, remote access, incident reporting and end-of-support arrangements.

Table 4 translates specialist terms into requirements that a procurement team can understand and test. For example, a requirement for multi-factor authentication means that a password alone is not enough for sensitive access. A 30-day repair period for a critical vulnerability means that the supplier must provide a fix or approved mitigation within that period. These clauses should be adapted to the nature of the device and the clinical risk; a life-support system may require a carefully controlled maintenance window rather than an automatic update.

Procurement area	Requirement written in clear language	Technical issue addressed
Authentication	The product must not contain fixed or hard-coded passwords. Sensitive access must require at least two independent forms of verification.	Prevents weak identity checks and built-in credentials (CWE-287 and CWE-798).
Data protection	Information sent across a network must be strongly encrypted. Stored information must also be encrypted using an accepted current standard.	Prevents confidential information from being transmitted or stored in readable form.
Patching and repairs	The supplier must repair a critical security weakness within 30 days, or provide an approved temporary safeguard. The normal update cycle must not exceed 90 days unless clinical safety requires a documented exception.	Reduces the period during which known weaknesses remain exploitable. CVSS 9.0 or above means a vulnerability is rated critical.
Cybersecurity warranty	At delivery, the equipment must be free from publicly known unaddressed critical vulnerabilities. The supplier must provide security updates and incident support for the agreed service life.	Closes the common gap between purchase, maintenance and long-term update support.

Table 4. Example procurement clauses written for managers, procurement officers and non-technical readers.

8. Discussion: Barriers and Enablers

Several barriers will affect implementation. Healthcare budgets are under pressure, and security spending competes with staffing, medicines and equipment. Many devices operate on old platforms that cannot be patched without downtime or

recertification. Smaller and rural providers often have fewer security specialists and less capacity to negotiate with large suppliers. These constraints mean that an ideal technical solution may be unrealistic.

However, improvement does not always require a complete replacement programme. A reliable asset inventory, network segmentation, stronger access control and better contract language can reduce risk at comparatively modest cost. Shared services can provide monitoring and incident-response support to smaller facilities. Standardised assessments allow management to compare departments using evidence rather than relying on the loudest concern or the most recent incident.

Artificial intelligence and machine learning may support anomaly detection across large volumes of network and device data. Their value lies in helping analysts notice patterns that would otherwise be missed. They should not be presented as autonomous solutions. Models can produce false alarms, miss unfamiliar activity or become less reliable as normal clinical behaviour changes. Human oversight, testing and clear accountability remain essential.

9. Recommendations

1. Create a single cross-functional cybersecurity governance committee with authority across information technology, operational technology, clinical engineering, procurement, legal services and senior management.

2. Maintain a complete and regularly updated inventory of connected medical devices, applications, cloud services, suppliers, software versions, data flows and remote-access arrangements.

3. Use one consistent risk-assessment method across IT and OT, while giving additional weight to patient safety, clinical disruption and the difficulty of replacing or patching equipment.

4. Segment clinical and administrative networks using controlled zones and connections. High-risk devices such as infusion pumps, imaging systems and hospital information systems should receive priority.

5. Include measurable cybersecurity requirements in every relevant tender and contract. Requirements should cover identity verification, encryption, patching, vulnerability disclosure, incident reporting, secure remote access and support at the end of the product's life.

6. Adopt continuous monitoring that brings together IT, OT, IoMT and supplier-related events. Analytics may assist detection, but decisions that could interrupt clinical services should remain subject to authorised human review.

7. Develop shared security services, training and incident-response support for smaller, rural and resource-constrained providers.

8. For Nigerian organisations, align implementation with the Nigeria Data Protection Act, applicable health-sector rules, public-procurement procedures and national cybersecurity guidance, while using NIST, ISO and IEC standards as technical reference points.

10. Conclusion

Connected healthcare systems have improved the speed, reach and quality of care, but they have also linked information systems, medical devices and operational infrastructure in ways that create shared cyber risk. The evidence reviewed in this paper shows that known device weaknesses remain common, security requirements are often missing from procurement documents, and fragmented governance allows a local weakness to become an organisation-wide problem.

The appropriate response is not another isolated security product. Healthcare organisations need a common operating model that begins with asset visibility, applies consistent risk assessment, assigns clear accountability and protects the continuity of patient care. The four-layer framework proposed here offers that structure. It combines recognised international standards with practical steps that hospitals can adopt gradually, beginning with their

highest-risk systems and most important suppliers.

Future work should test the framework in different healthcare settings, including Nigerian tertiary hospitals, state facilities and smaller rural providers. Evaluation should measure not only technical detection rates, but also procurement compliance, response time, service continuity and patient-safety outcomes.

Glossary of Key Terms

Term	Meaning
AI	Artificial intelligence: computer systems that perform tasks such as pattern recognition or prediction.
AES-256	A widely used method for encrypting stored data.
CSET	Cybersecurity Evaluation Tool: a structured method for assessing an organisation's security.
CTI	Cyber threat intelligence: information about attackers, methods, vulnerabilities and indicators of compromise.
CWE	Common Weakness Enumeration: a catalogue of recurring software and hardware weaknesses.
CVSS	Common Vulnerability Scoring System: a 0-10 scale used to describe how serious a vulnerability is.
IoMT	Internet of Medical Things: connected medical devices and healthcare sensors.
IT	Information technology: data, applications, servers and communications systems.
OT	Operational technology: equipment and systems that monitor or control physical processes.
SIEM	Security Information and Event Management: a platform that gathers and analyses security logs.
SOAR	Security Orchestration, Automation and Response: tools that coordinate and automate approved incident-response tasks.
TLS 1.3	A current security protocol used to protect data while it travels across a network.
Zero Trust	An access model in which every user, device and request is verified rather than automatically trusted.

References

Akram, M., Khan, W., Rasheed, M. D., Imran, M., Iqbal, M. W., Delshadi, A., & Sultana, M. (2026). Cybersecurity risk assessment model for Internet of Medical Things (IoMT) devices in healthcare systems. Spectrum of Engineering Sciences, 4(3), 312-326. https://doi.org/10.5281/zenodo.18951916

Bacula Systems. (2026). IEC 62443 standard and security levels: A complete OT guide. https://www.baculasystems.com/blog/iec-62443-security-standard/

Claroty. (2025). What is the ISA/IEC 62443 framework? https://claroty.com/blog/what-is-the-isa-iec-62443-framework

Cybersecurity and Infrastructure Security Agency. (2023). Cybersecurity advisories. U.S. Department of Homeland Security. https://www.cisa.gov/news-events/cybersecurity-advisories

European Union Agency for Cybersecurity. (2023). ENISA threat landscape: Health sector. https://www.enisa.europa.eu/publications/health-threat-landscape

Filani, A., Addotey, N., & Opoku, J. A. (2026). Cybersecurity threat landscape in the US healthcare sector: Trends, risks, and national implications. International Journal of Technology and Applied Science, 17(1), 1-12.

Health-ISAC. (n.d.). About Health-ISAC. https://health-isac.org

HIPAA Journal. (2025, October 26). Healthcare data breach statistics. https://www.hipaajournal.com/healthcare-data-breach-statistics/

IBM. (2025). Cost of a data breach report 2025. IBM Security.

İmamoğlu, M. B. (2025). Cyber infrastructure guide: IT/OT integration. Ömer Halisdemir Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 18(1), 378-391. https://doi.org/10.25287/ohuiibf.1558269

International Organization for Standardization. (2016). ISO 13485:2016: Medical devices - Quality management systems - Requirements for regulatory purposes.

International Organization for Standardization. (2019). ISO 14971:2019: Medical devices - Application of risk management to medical devices.

International Organization for Standardization. (2022a). ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection - Information security management systems - Requirements.

International Organization for Standardization. (2022b). ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection - Information security controls.

International Society of Automation. (2018). ISA/IEC 62443 series of standards: Industrial automation and control systems security.

Mengnjo, G. B. (2026). Assessing healthcare supply chain cybersecurity using the Cybersecurity Self-Evaluation Tool (CSET) [Doctoral dissertation, Capitol Technology University].

MITRE Corporation. (n.d.). CWE - Common Weakness Enumeration. https://cwe.mitre.org

National Institute of Standards and Technology. (2020). Zero trust architecture (NIST Special Publication 800-207). https://doi.org/10.6028/NIST.SP.800-207

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

Nozomi Networks. (2026). ISA/IEC 62443 standards: Best practices for IACS cybersecurity.

Pandey, S., & Kumar, R. (2026). Analysing cybersecurity gaps in medical device procurement using NLP and vulnerability databases. Discover Internet of Things, 6(9). https://doi.org/10.1007/s43926-025-00279-2

Tesserent. (2024). What is IEC 62443? IEC 62443 standard explained.

U.S. Department of Health and Human Services. (1996). HIPAA Security Rule (45 CFR Part 160 and Subparts A and C of Part 164).

U.S. Department of Health and Human Services 405(d) Program. (2023). Health industry cybersecurity practices: Managing threats and protecting patients.

U.S. Food and Drug Administration. (2023). Cybersecurity in medical devices: Quality system considerations and content of premarket submissions.