



MEDICAL IOT THREAT MODELING: A LIFECYCLE-BASED FRAMEWORK FOR INTEGRATING CYBERSECURITY RISK AND PATIENT SAFETY

Adewumi Busayo Adelemi *

Division of Engineering and Computer Science, Cybersecurity, Oklahoma Christian University.

* Corresponding Author

International Journal of Science and Research Archive, 2026, 21(01), 176–180

Publication history: Received on 29 August 2026; revised on 04 October 2026; accepted on 06 October 2026

Article DOI: <https://doi.org/10.30574/ijrsra.2026.21.1.1852>

Copyright © 2026 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0

ABSTRACT

Connected medical devices, including infusion pumps, patient monitors, implantable devices, and remote monitoring platforms, have expanded the attack surface of modern healthcare delivery beyond what traditional IT security practices were designed to address. This paper's objective is to examine threat modeling as a structured, lifecycle-based discipline for identifying and mitigating cybersecurity risks specific to medical Internet of Things (IoMT) devices, and to argue that patient-safety impact must be integrated explicitly into existing threat-modeling methodologies rather than treated as a secondary concern. The methodology consisted of a targeted literature and documentation review covering regulatory guidance, peer-reviewed security research, and documented device vulnerability cases, combined with an applied walkthrough of established threat-modeling methodologies (STRIDE, DREAD, PASTA, and attack-tree analysis) against a representative device scenario. Results show that generic IT threat-modeling approaches underweight safety-critical consequences and do not account for the extended regulatory lifecycles, legacy protocols, and patch constraints characteristic of medical devices, and that documented real-world cases, including confirmed vulnerabilities in implantable cardiac devices, demonstrate that these risks are not theoretical. The paper concludes that threat modeling delivers the most value when applied continuously across a device's full lifecycle, from procurement through post-deployment monitoring, and when existing scoring methodologies are explicitly adapted to weight patient-safety severity. Future work should focus on standardized, patient-safety-weighted scoring extensions and empirical evaluation of threat-modeling programs in real hospital deployments.

Keywords: Medical Iot Security; Threat Modeling; STRIDE; Patient Safety; Medical Device Cybersecurity

1 INTRODUCTION

Healthcare delivery organizations have become one of the most heavily targeted sectors in cybersecurity, and the reasons are structural rather than incidental. Hospitals combine high-value data (protected health information, insurance and billing records), safety-critical operational technology, and historically under-resourced security functions, producing an environment where the cost of a successful attack, in both financial and patient-safety terms, is unusually high. Within this environment, the growth of medical Internet of Things (IoMT) devices has introduced a category of risk that neither general enterprise IT security practices nor traditional medical device safety engineering was built to address on their own.

IoMT devices differ from conventional IT assets in several important ways. Many run on embedded operating systems that can't be patched without vendor involvement or regulatory re-approval. Their operational lifespans frequently exceed a decade, meaning devices deployed under one generation of security assumptions remain in clinical use long after those assumptions have become obsolete. Their primary function is patient care, so availability and safety take precedence over confidentiality in ways that complicate standard risk triage. And because many of these devices interact directly with patients, administering medication, monitoring vital signs, or controlling implanted hardware, a security failure can translate directly into physical harm, not merely data loss.

Threat modeling offers a structured method for anticipating these risks before they're exploited: identifying how an asset could be attacked, what the consequences would be, and where mitigating controls should be placed. This paper reviews the case for applying threat modeling specifically to medical IoT devices, surveys applicable methodologies, works through an illustrative example, and discusses how the practice should be integrated across a device's operational lifecycle.

2 MATERIALS AND METHODS

This paper is a narrative literature and documentation review rather than an empirical study, and no primary data were collected from human or animal subjects. Sources were identified through targeted searches of peer-reviewed security literature (via IEEE Xplore and related academic databases), official regulatory guidance and safety communications (U.S. Food and Drug Administration and CISA/ICS-CERT medical advisories), and foundational primary texts documenting established threat-modeling methodologies (STRIDE, DREAD, PASTA, and attack-tree analysis). Sources were selected for direct relevance to medical device or medical IoT security and for methodological authority (originating standards documents, regulatory communications, or peer-reviewed research in preference to secondary summaries). The selected methodologies were then applied narratively to a representative, illustrative device scenario (a networked infusion pump) to demonstrate how each methodology surfaces device-specific threats, and the resulting findings were synthesized into lifecycle-stage recommendations for when and how threat modeling should be applied in a hospital setting.

3 RESULTS AND DISCUSSION

3.1 Documented Vulnerabilities and Regulatory Context

Security researchers and regulators have documented vulnerabilities across many medical device categories, from infusion pumps and insulin pumps to implantable cardiac devices, imaging systems, and hospital-grade wireless monitors. Recurring weaknesses identified in the literature include hardcoded or default credentials, unencrypted communication protocols, absence of secure boot or firmware-signing mechanisms, and insufficient network segmentation between clinical devices and the broader hospital IT network [1]. Regulatory bodies such as the U.S. Food and Drug Administration (FDA) have progressively introduced premarket and postmarket cybersecurity expectations for connected medical devices. This shift reflects a growing recognition that device security can no longer be treated as separate from device safety [2].

Documented cases illustrate the real-world consequences of these weaknesses. In 2017, the FDA confirmed that certain radio-frequency-enabled implantable cardiac pacemakers manufactured by St. Jude Medical (later acquired by Abbott) contained vulnerabilities that, if exploited, could allow an unauthorized user to alter the paired Merlin@home monitoring transmitter and issue unauthorized commands to the implanted device, with potential consequences including rapid battery depletion or inappropriate pacing [3]. A corrective firmware update was subsequently issued later that year, requiring an in-clinic visit to apply [4].

Prior work on applying structured threat modeling and risk assessment to safety-critical embedded systems more broadly, including landmark security research on automotive systems and reviews of industrial control system (SCADA) risk assessment methods, provides methodological precedent [5], though healthcare-specific adaptation of scoring models such as DREAD to properly weight patient-safety impact remains an area with comparatively limited published literature.

3.2 Why Generic IT Threat Models Fall Short for IoMT

Standard IT threat modeling assumes a degree of flexibility, frequent patch cycles, replaceable hardware, and confidentiality-first risk prioritization, that doesn't hold for most medical devices. Four constraints distinguish IoMT threat modeling from conventional enterprise threat modeling:

- **Safety-criticality:** An attack that alters device behavior (e.g., dosage delivered by an infusion pump) can cause direct physical harm, which changes how likelihood and impact should be scored relative to a typical data-breach scenario.
- **Legacy protocols and embedded constraints:** Many devices use lightweight or proprietary communication protocols not designed with modern cryptographic protections, and limited computing/memory headroom restricts what security controls can even be added post-hoc.
- **Patch and change-control constraints:** Firmware changes to a regulated medical device may require vendor involvement and, in some cases, regulatory re-approval, making rapid remediation far slower than in general IT.
- **Extended regulatory lifecycle:** Devices are frequently approved, deployed, and supported over multi-year or multi-decade horizons, during which the threat landscape changes substantially while the device's security architecture may not.

3.3 Applicable Methodologies

Several established threat modeling methodologies can be adapted to the IoMT context, each contributing a different lens:

- **STRIDE** (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege), originally developed by Kohnfelder and Garg at Microsoft in 1999 and later formalized within Microsoft's Security Development Lifecycle [6], provides a systematic checklist for categorizing threats against a device's data flows and trust boundaries, useful for enumerating how an attacker might interact with a device's communication interfaces (Bluetooth, Wi-Fi, USB, cellular).
- **DREAD** (Damage, Reproducibility, Exploitability, Affected Users, Discoverability) offers a scoring approach for prioritizing identified threats, though in a clinical context "Damage" should explicitly incorporate patient-safety severity, not just data or financial impact.
- **PASTA** (Process for Attack Simulation and Threat Analysis), a seven-stage risk-centric methodology developed by UcedaVélez and Morana [7], ties technical threat identification back to business/clinical objectives and compliance requirements, making it well suited to hospital environments where security decisions must be justified against clinical and regulatory priorities.
- **Attack trees**, formalized by Schneier [8], provide a visual, hierarchical decomposition of how an adversary could achieve a specific goal (e.g., "alter medication dosage remotely"), which is particularly effective for communicating risk to clinical and executive stakeholders who aren't security specialists.

In practice, mature IoMT threat-modeling programs tend to combine STRIDE-style enumeration for coverage with PASTA-style business/clinical framing for prioritization, using attack trees as a communication artifact for specific high-concern scenarios.

3.4 Emerging Case: Brain-Computer Interfaces

Implantable brain-computer interfaces (BCIs), such as Neuralink's investigational device, represent an emerging IoMT category that extends threat modeling into a substantially higher-stakes domain than conventional connected medical devices. Commentary on BCI security has flagged wireless connectivity, particularly the link between an external companion application and the implant, as a likely weak point, since a compromised companion app could in principle be used to send unauthorized commands to the implant or expose recorded neural data [9]. This concern is consistent with earlier, empirically demonstrated research on other implantable devices: Halperin et al. showed that an implantable cardiac defibrillator could be attacked via software radio to compromise patient privacy and device state, and Radcliffe demonstrated at Black Hat USA 2011 that he could wirelessly reprogram and remotely disable his own insulin pump [10]. Because BCIs process neural signals rather than only conventional health data, the confidentiality dimension of a STRIDE-style analysis (Information Disclosure) must be extended to cover inferred cognitive or emotional states, not merely identifiable health records, a scope beyond what existing methodologies were originally designed to capture and an area future extensions of STRIDE/DREAD for IoMT should address explicitly.

3.5 Worked Example: A Networked Infusion Pump

Consider a hypothetical networked infusion pump connected to the hospital's wireless network for remote dosage monitoring and drug-library updates. A STRIDE-based walkthrough of its primary data flows might surface the following illustrative threats:

- **Spoofing:** An attacker on the same network segment impersonates the central pharmacy server pushing drug-library updates, potentially delivering a malicious dosage configuration.
- **Tampering:** Unencrypted or weakly authenticated firmware update mechanisms allow modification of pump software in transit.

- **Denial of Service:** Flooding the pump's network interface disrupts its ability to report status to clinical staff, potentially delaying detection of a dosage anomaly.
- **Elevation of Privilege:** A maintenance/debug interface left enabled in production allows an attacker with local network access to reach configuration functions not intended for clinical users.

Each identified threat would then be scored (e.g., via DREAD, with "Damage" weighted for patient-safety severity), mapped to existing or missing mitigations (network segmentation, mutual TLS authentication, signed firmware updates, disabling of debug interfaces), and tracked through to remediation ownership, typically a shared responsibility between the hospital's clinical engineering/biomedical team and the device vendor. This example is illustrative and generic, not based on a specific real-world incident or product.

3.6 Integration Across the Device Lifecycle

Threat modeling delivers the most value when it is not a one-time exercise, but a recurring process aligned to the device lifecycle:

- **Design/procurement time:** evaluating vendor security posture and device architecture before purchase, ideally using threat-modeling findings as a factor in vendor selection.
- **Deployment/integration time:** assessing how the device interacts with the hospital's specific network topology, since the same device can present different risk depending on segmentation and surrounding infrastructure.
- **Continuous post-deployment review:** reassessing as new vulnerabilities are disclosed, as the device ages, or as its clinical use context changes.

Hospitals with mature biomedical/clinical engineering functions increasingly treat threat modeling as an input to procurement decisions and ongoing asset management, not merely a post-purchase compliance exercise. Embedding threat-modeling outputs into the hospital's asset inventory and risk register (functions typically owned by the organization's broader security governance program) is what allows individual device assessments to remain relevant over time rather than becoming static, one-off artifacts.

Limitations

Several practical limitations constrain the adoption of structured threat modeling for medical IoT devices. First, resource constraints are significant in many healthcare delivery organizations, particularly smaller or rural hospitals, where dedicated security and clinical-engineering staff capable of performing structured threat modeling may not exist. Second, the extended lifecycle of medical devices means threat models must be revisited periodically, which requires sustained institutional commitment rather than a one-time project. Third, vendor cooperation is often necessary for remediation (firmware updates, architecture changes), and hospitals frequently lack contractual leverage to compel timely vendor action. Finally, existing threat-modeling methodologies (STRIDE, DREAD, PASTA) weren't designed specifically for safety-critical clinical devices, and adapting their scoring dimensions to properly weight patient-safety impact remains more art than standardized science.

4 CONCLUSION

Medical IoT devices introduce risk characteristics, safety-criticality, embedded constraints and long regulatory lifecycles, that generic IT threat modeling doesn't fully address without adaptation. This paper has reviewed how established methodologies (STRIDE, DREAD, PASTA, attack trees) can be adapted to the clinical context, illustrated their application through a representative device example, and discussed the importance of integrating threat modeling across the full device lifecycle rather than treating it as a one-time exercise. Future work should focus on empirical evaluation of threat-modeling programs in real hospital deployments, development of standardized patient-safety-weighted scoring extensions to existing methodologies, and research into scalable, low-resource threat-modeling approaches suitable for smaller healthcare delivery organizations that can't support dedicated security teams.

STATEMENTS ON COMPLIANCE WITH ETHICAL STANDARDS

Disclosure of conflict of interest

The author declares no conflict of interest.

REFERENCES

- [1] Ghubaish A, Salman T, Zolanvari M, Unal D, Al-Ali A, Jain R. Recent advances in the internet-of-medical-things (IoMT) systems security. *IEEE Internet Things J.* 2021;8(11):8707-18.
- [2] U.S. Food and Drug Administration. Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions. Guidance for Industry and Food and Drug Administration Staff. Silver Spring (MD): FDA; 2026 Feb 3.
- [3] U.S. Food and Drug Administration. Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication. Silver Spring (MD): FDA; 2017 Jan 9.
- [4] U.S. Food and Drug Administration. Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication. Silver Spring (MD): FDA; 2017 Aug 29.
- [5] Miller C, Valasek C. Remote Exploitation of an Unaltered Passenger Vehicle. Seattle (WA): IOActive; 2015. Presented at: Black Hat USA; 2015; and Cherdantseva Y, Burnap P, Blyth A, Eden P, Jones K, Soulsby H, Stoddart K. A review of cyber security risk assessment methods for SCADA systems. *Comput Secur.* 2016; 56:1-27.
- [6] Kohnfelder L, Garg P. The Threats to Our Products. Redmond (WA): Microsoft; 1999. Internal document, later formalized in Microsoft's Security Development Lifecycle; see also Shostack A. *Threat Modeling: Designing for Security.* Indianapolis (IN): Wiley; 2014.
- [7] UcedaVélez T, Morana MM. *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis.* Hoboken (NJ): Wiley; 2015.
- [8] Schneier B. Attack trees. *Dr Dobbs J.* 1999;24(12):21-9.
- [9] Bocetta S. What are the security implications of Elon Musk's Neuralink? *CSO Online.* 2019 Aug 1.
- [10] Halperin D, Heydt-Benjamin TS, Ransford B, Clark SS, Defend B, Morgan W, Fu K, Kohno T, Maisel WH. Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses. In: *Proc 2008 IEEE Symp Secur Priv.* 2008 May:129-42; and Radcliffe J. Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System. Presented at: Black Hat USA; 2011 Aug.