A STRIDE-based Threat Modeling Framework for Small Clinics and AI-Enabled Healthcare Services

Sri Sowmya Nemani
Junior Security Analyst

ABSTRACT
Small clinics operate medical devices (imaging, anesthesia monitors), EHR systems, payment terminals, and third-party integrations (diagnostic labs, suppliers). Despite handling sensitive client data and relying on networked medical devices, these clinics rarely adopt formal threat-modeling practices. This paper presents the Threat modeling for small scale businesses like Vet clinics, Chiropractor clinics, AI-Enabled Health care service etc. Mostly, lightweight STRIDE threat modeling for IoT and EHR security. This paper demonstrates the framework on a representative clinic profile and shows how straightforward mitigations (TLS, MFA, network segmentation, vendor contract clauses) measurably reduce attack surface and risk exposure.

Keywords
EHR (electronic Health Record), IoT (Internet of Things), AI (Artificial Intelligence)

1. INTRODUCTION
Protecting both digital and physical assets is important. STRIDE is a structured threat-modeling methodology originally developed by Microsoft to help analysts systematically identify and categorize security threats during system design and assessment.[1] [12]

STRIDE represents six key threat classes — Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege.[2] [4][11]

This paper proposes a STRIDE-based threat-modeling framework tailored for small veterinary clinics. The model integrates IoT device security, EHR data protection, and third-party vendor dependencies into a unified threat landscape.

2. RESEARCH QUESTION
How can the STRIDE threat-modeling methodology be adapted and applied to small clinics, AI-enabled healthcare startups to identify cybersecurity threats affecting IoT medical devices, EHR systems, and third-party integrations and NLP-based clinical workflows.

3. EVOLVING IN SAAS BASED HEALTHCARE SYSTEMS
Over the past five years, a growing number of healthcare organizations and small clinics have shifted from on-premises Electronic Health Record (EHR) systems to cloud-hosted Software-as-a-Service (SaaS) platforms. Many vendors provide AI augmented tools for patient management, billing, diagnostics and telehealth. Most SaaS-based healthcare systems store sensitive Protected Health Information (PHI) and Personally Identifiable Information (PII) in multi-tenant cloud environments. The data includes:

- Patient demographics, diagnosis codes, billing records
- IoT data streams (vitals, device telemetry) synced from medical sensors
- Diagnostic files such as DICOM images, lab results, and scanned prescriptions
- Predictive models trained on clinical data (AI models with embedded PHI risk)

Unlike traditional EHR setups where the clinic retains full data control, SaaS applications often rely on shared responsibility models. Cloud providers secure the underlying infrastructure, while clinics are responsible for identity, access, and configuration management. Misconfigurations, weak API authentication, or unvetted AI model training can cause unintentional data leakage or model inversion attacks. Furthermore, AI-enabled SaaS systems in healthcare frequently use third-party APIs for OCR (optical character recognition), NLP-based clinical summarization, or diagnostic prediction. These integrations expand the attack surface:

- API exposure: Weak API keys, poor rate limiting, or lack of TLS 1.3 encryption.
- Data residency risk: Data stored across jurisdictions (HIPAA vs. GDPR conflicts).
- Model poisoning: Threat actors injecting manipulated training data through connected devices or uploads.
- Auditability gap: Limited visibility into how SaaS vendors process, store, and delete PHI.

3.1 CASE STUDY
Page Community Veterinary Clinic is a small, ten-staff veterinary practice in Long Island that relies on IoT medical devices, a cloud-based EHR system, and multiple third-party vendors for diagnostics and pharmacy services. The clinic handles sensitive client, payment, and medical data but operates with minimal formal security controls, no strong password policy, no disaster-recovery plan, and limited staff training. This makes it representative of many small clinics that depend heavily on SaaS tools and vendor integrations but lack dedicated IT teams. The case study provides a realistic environment to apply the STRIDE framework and demonstrates how lightweight threat modeling can identify key risks and guide practical, low-cost security improvements.

4. METHODOLOGY
This study adopts a STRIDE-based threat-modeling methodology tailored to the operational realities of small clinics, including veterinary clinics, chiropractic offices, and outpatient care centers. According to OWASP Threat Modeling we must consider four questions when designing a model like [6] What are we working on? What can go wrong? What are we going to do about it? Did we do a good job? The methodology follows a structured, repeatable workflow: (1)

system scoping and asset identification, (2) data-flow diagramming, (3) STRIDE-driven threat enumeration, and (4) Threat mitigations. Unlike heavyweight enterprise threat-modeling frameworks, this approach is intentionally lightweight, enabling small clinics—often without dedicated IT or security teams—to perform meaningful risk analysis with minimal overhead.

4.1 SYSTEM SCOPING AND ASSET IDENTIFICATION

First phase involves identifying inventory and assets list

Table-1 Asset Identification

Devices	Details
IoT Medical Devices	Imaging systems, anesthesia monitors, vital-sign sensors, and diagnostic modules connected to the clinic network.
Cloud-Based EHR	SaaS EHR platforms that store Protected Health Information (PHI) and provide billing, scheduling, and clinical documentation functionality
Third Party Integrations	Diagnostic laboratories, pharmacies, radiology centers, AI-based OCR/NLP APIs, and telehealth service providers.
Network Infrastructure	Consists of Wi-Fi routers, switches, point-of-sale (POS) terminals, staff workstations, and administrative devices.

Categorizing the technical ecosystem of clinics. Each asset was evaluated using confidentiality, integrity, and availability (CIA) requirements to determine potential risk impact.[2] [12]

4.2 Data Flow Diagram

We apply each STRIDE category to every data flow and asset class. This paper expands traditional STRIDE by explicitly including AI-enabled SaaS integrations and third-party clinical APIs, which now play a central role in modern clinic operations. AI-Enabled SaaS and Third-Party APIs as Emerging Threat Vectors many small clinics rely on cloud EHR vendors that bundle AI-driven services such as:

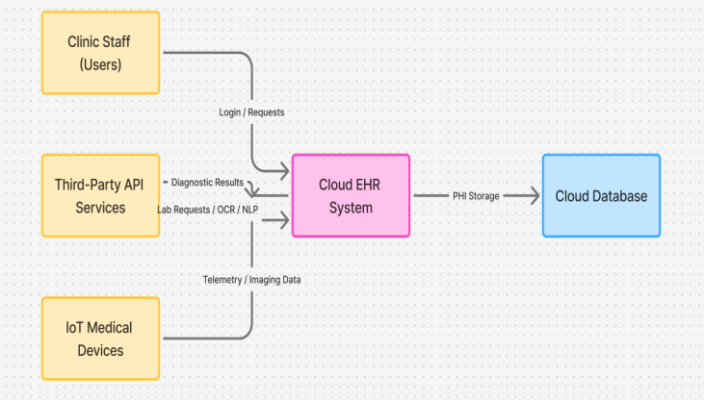

Fig 1: Data Flow Diagram

- OCR engines for converting scanned prescriptions or intake forms.
- NLP summarization tools that auto-generate visit notes.
- Diagnostic prediction APIs that process imaging or lab data.
- Billing AI models trained on PHI.
- Telehealth voice-to-text transcription and analysis. Each AI integration expands the attack surface by introducing new trust boundaries and external dependencies.

4.3 STRIDE-Based Threat Enumeration

STRIDE was applied to every data flow, asset category, and trust boundary. Threats were identified across IoT telemetry, EHR authentication, vendor communications, and API operations. [2]

- **Spoofing:** Threats arise mainly from stolen credentials, insecure logins and third-party APIs to AI services.
- **Tampering:** Concerns involve manipulation of IoT Sensor Data, altered clinical Documentation produced by NLP systems.
- **Repudiation:** Improper logging makes it difficult to verify user actions within the AI generated records.
- **Information Disclosure:** PHI exposure from misconfigured cloud storage, intercepted API traffic, OCR pipelines, and unintended leakage from AI model outputs.
- **Denial of Service (DoS)** Threats like network interruptions, API flooding.
- **Elevation of Privileges:** System Misconfigurations or RBAC settings to gain admin level access.

4.4 EXAMPLE INDUSTRY

This study considers anonymized examples of modern AI-enabled healthcare service providers. These organizations operate across mobile diagnostics, virtual care, and EHR-integrated documentation platforms. Many of these organization models mirror several well-known industry solutions in remote care, on-demand health services, and AI-driven clinical automation.

Table -2 Mapping

Service Type	Components	STRIDE Threat
Mobile at-home care	NLP Visit Summary	Tampering
Remote Diagnostics and Patient Monitoring	OCR extraction and ML anomaly Detection	Information Disclosure and Tampering
EHR- Integrated AI Scribe	LLM Summarization	Spoofing
Telehealth	Symptom NLP	DoS

4.5 THREAT MITIGATION

STRIDE analysis conducted across IoT devices, cloud-based EHR systems, third-party APIs, and AI/NLP-driven clinical workflows, the following mitigation strategies are recommended for small clinics and AI-enabled healthcare startups.[2] [10]

Table-3 Threat Mitigation

Category	Threat Scenario	Mitigations
AI/NLP Clinical Workflows.	• Adversarial text poisoning. •Manipulated OCR/NLP inputs. • PHI leakage from LLM outputs. • Model inversion attacks. • Spoofed AI API calls.	• Input validation & adversarial filtering. • Output PHI-scrubbing & redaction.
IOT Medical Devices	• Tampered vital-sign readings • Fake sensor values •Unauthorized firmware changes • Wireless interception	• Secure boot and signed firmware updates • Encrypted wireless protocols (WPA3, BLE-E, DTLS)
Cloud-Based EHR Systems	• Weak login security • PHI exposure • Privilege escalation •Misconfigurations	• MFA and short-lived tokens • RBAC & least-privilege controls
Remote Diagnostics	• Spoofed API clients • Insecure mobile apps • Excessive data sharing • Vendor breaches	• Vendor risk assessments and PHI handling reviews • Data minimization (only required PHI transmitted)
Human Controls	• Phishing • Credential misuse • Ransomware • Lack of security awareness	•Cybersecurity training for staff • Offline + cloud backups • Disaster recovery plan (DRP)

5. RELATED WORK

Recent literature has explored the intersection of artificial intelligence, electronic health records (EHR), clinical documentation, and IoT-enabled medical systems. These studies highlight how important it is to integrate AI with the EHR data and risk associated with modernizing healthcare workflows.

Firstly, the research focuses on integrating AI with EHR System to enhance predictive care. A recent study by Ahmed et al. (2024) [7] demonstrated how AI-driven analytics can enable early detection of health conditions, improve diagnostic accuracy, and support more precise treatment planning. Although AI-enhanced EHR systems offer significant improvements in efficiency and clinical insight, the study also noted that such integrations remain in early stages due to unresolved concerns around data privacy, PHI governance, and regulatory compliance such as HIPAA (Ahmed et al., 2024).[7]

Another research work has examined challenges surrounding clinical documentation. According to Imran et al. (2024),[8] physicians spend between 34% and 55% of their workday creating and reviewing clinical documentation within EHR systems, representing a national opportunity cost of approximately $90 to $140 billion annually. These findings further illustrate the increasing need for AI-assisted documentation tools—such as NLP-based note summarizers—to reduce clinician workload, although these tools introduce new risks related to accuracy, integrity, and auditability.[8]

In parallel, this research work talks about security implications of incorporating AI into healthcare systems. Saini et al. (2025)[9] discuss how AI integration introduces risks such as algorithmic opacity, data breaches, and vulnerabilities in AI-controlled medical devices. Their work highlights the importance of CRM (Clinical Risk Management) in preventing system level failures and managing threats.

More closely aligned with the current paper, Zhang et al. (2025)[10] conducted a qualitative and quantitative security assessment of 23 IoT healthcare devices using the STRIDE and DREAD models. Their work demonstrates how traditional threat-modeling frameworks can be applied to medical IoT ecosystems. However, their focus remains primarily on device-level IoT threats and does not address emerging risks associated with AI-driven EHR workflows, NLP-based clinical automation, or third-party healthcare APIs used in modern small-clinic and startup ecosystems.[10]

6. CONCLUSION

This paper shows that STRIDE is a practical and easy-to-use method for helping small clinics understand their cybersecurity risks. As more clinics rely on cloud EHR systems, IoT medical devices, and AI-based tools for documentation and diagnostics, their attack surface grows in ways they may not expect. By mapping out how data moves between devices, applications, and vendors, the STRIDE model highlights common issues such as weak authentication, unprotected data flows, insecure IoT sensors, and risks created by NLP and third-party APIs.

Small clinics can greatly reduce risk by using basic controls like MFA, encryption, network segmentation, and stronger vendor rules—none of which require large budgets. This STRIDE approach can also be applied to telehealth, mobile health, and AI-driven services. More research is needed to understand how AI and LLM tools impact data accuracy and security in real clinical environments.

7. REFERENCES

[1] McCoy, D. (2025, February 2). Understand all things cybersecurity, EHR, and spam [Audio podcast episode]. Chiro Hustle Podcast, Episode 703.

[2] Hossain, M. I., & Hasan, R. (2024). Improving security practices in health information systems with STRIDE threat modeling. IEEE WF-IoT.

[3] Zhai, B., Akande, O. N., Agarwal, S., & Pak, W. (2025). Security considerations in digital healthcare ecosystems. ScienceDirect.

[4] U.S. Department of Health and Human Services. (2023).Threat modeling for mobile health systems. https://www.hhs.gov

[5] Alozie, C. (2024). Threat modeling in the health care sector. https://www.researchgate.net/publication/389100717_Threat_Modeling_in_Health_Care_Sector

[6] OWASP. (n.d.). Threat modeling. https://owasp.org/www-community/Threat_Modeling

[7] Ahmed, S., Kumar, R., & Banerjee, A. (2024). Automating healthcare with AI: Optimizing electronic health records and predictive analytics for improved patient outcomes. https://www.researchgate.net/publication/390761189_Automating_Healthcare_with_AI_Optimizing_Electronic_Health_Records_and_Predictive_Analytics_for_Improved_Patient_Outcomes

[8] Imran, M., Kelley, L., & Torres, J. (2024). Enhancing clinical documentation efficiency using advanced EHR systems. https://pmc.ncbi.nlm.nih.gov/articles/PMC11605373/

[9] Saini, R., Gupta, P., & Lee, D. (2025). AI integration in healthcare: Risks, vulnerabilities, and clinical risk management considerations. Journal of Medical Systems. https://pmc.ncbi.nlm.nih.gov/articles/PMC12579840/

[10] Zhang, Y., Chen, H., & Mohammed, S. (2025). Security assessment of IoT-based health devices using STRIDE and DREAD. Digital Communications and Networks. https://www.sciencedirect.com/science/article/pii/S2090447925004629

[11] Chandra, S., Kalra, A., & Gupta, R. (2023). Security and privacy challenges in AI-enabled healthcare systems. Journal of Healthcare Informatics Research.

[12] Kumar, P., & Singh, A. (2024). Risk assessment and mitigation strategies in cloud-based healthcare platforms. International Journal of Medical Informatics.