INSTITUTE FOR HOMELAND SECURITY

Emerging Threats Against Urgent Care Centers

Institute for Homeland Security

Sam Houston State University

Narasimha Karpoor Shashidhar and Cihan Varol

Emerging Threats Against Urgent Care Centers

Narasimha Karpoor Shashidhar, and Cihan Varol
Digital Forensics and Information Assurance Lab
{karpoor, cxv007}@shsu.edu

Department of Computer Science
Sam Houston State University

Emerging Threats Against Urgent Care Centers

Narasimha Karpoor Shashidhar[1]*, and Cihan Varol[2]
Digital Forensics and Information Assurance Lab
{karpoor, cxv007}@shsu.edu
Department of Computer Science
Sam Houston State University
*Corresponding author

Table of Contents

[1] www.linkedin.com/in/karpoor
[2] https://www.linkedin.com/in/cihan-varol-53105012/

1. Abstract: Overview and Motivation

a. Scope and Methodology

Urgent care centers have become an essential aspect of everyday life in our modern society. Securing this critical healthcare infrastructure is, naturally, of paramount importance.

This report sheds light on some potentially insidious emerging threats of the next decade as they pertain to small and medium-sized businesses. In particular, *Urgent Care Centers* in Texas and the country. To this end, data has been collated using cyber security threat reports published by industry (Deloitte, CrowdStrike, Cisco, IBM, Verizon, Google, etc.) and government agencies (White House, NIST, Homeland Security, CISA, etc.) to put forth an educated guess on the nature and severity of cyberattacks that may plague this health-care sector of small and medium-sized businesses in the subsequent decade. In developing this report, the authors have considered nascent, upcoming technologies that are destined to become mainstream in the coming years. These include, but are not limited to Artificial Intelligence (AI), Generative AI, and Large Language Models, Cloud, Internet of Things, and the ever-changing geopolitical landscape of the world. Several physicians are drawn to the (lucrative) field of starting an urgent care center and while the cyber climate is favorable, everything seems rosy. It's only when a breach, or cyber-attack wreaks havoc do the urgent care proprietors begin to realize the dangers of an insecure cyber infrastructure. Unfortunately, in many instances, this realization may be too late.

To illustrate the gravity of these threats, the report also includes a graphic that captures the evolution and diversity of these attacks and the devastating impacts of such an attack on a typical urgent care center. This is done to impress upon the proprietors that while defense may cost some resources, being unprepared may be prohibitively expensive. The authors also briefly discuss cyber inequity and the impact of cybersecurity trends on society and economies in general in this context. This section of our report is also devoted to a brief discussion on regulatory mechanisms, risk management, assessment, and disaster recovery protocols.

Having identified this set of potential threats, the authors then outline tangible steps and measures that an urgent care SMB might proactively implement to insulate themselves against these threats. This report can serve as a prophylaxis against these upcoming threats. While not comprehensive, our intention is to help bolster health care centers against the most probable threat scenarios rather than all possible attacks. This is done with cost and time-efficiency in mind. Since most centers do not possess the means to devote substantial resources towards security, this report only includes options that can produce the most gain for their resources invested.

In summary, our report aims to inspire urgent care centers in Texas and around the country (that play a pivotal role in our modern society) to be mindful of the rapidly evolving landscape of cyber threats and attacks. This report brings to light our best forecast and predictions on the nature of cyber threats facing them in the next decade using reports from a diverse set of sources. Lastly, being proactive, this report will serve as a guide to be prepared and protected against some of these projected trends in threats and attacks for the next decade.

Keywords: urgent care, cybersecurity, risks, threats, mitigation, emerging threats, analysis.

2. Introduction

a. Background of Urgent Care Centers

Any discussion of urgent care centers in the U.S. necessarily must begin with the history and development of the primary care and general practitioner care model of medicine. Both these systems of care were borrowed from the United Kingdom dating back to the early 1900s. It is well known that the number of primary care physicians in the United States has steadily declined since 1950 and are in short supply. The reason for this decline is well documented [2]. To address this gap, urgent care centers have sprung up all over the country to alleviate this shortage in care givers. To learn more about the history of general practice in primary medical care, the interested reader is encouraged to read the National Academies Press report on the subject [1]. Urgent care centers are a relatively modern care system in the United States. A survey of the literature indicates that the first few urgent care centers were established around 1970 so as to fill the gap in primary care and to offer non-emergent care. These centers have almost always been opened by entrepreneurial doctors. Today, after the passage of the Affordable Care Act in 2010, these centers have become ubiquitous – particularly in an urban setting since many more Americans are now medically insured. It also comes as no surprise that COVID-19 has had an outsized influence on propelling the surge in growth of urgent care centers.

b. Need for and Importance of Threat and Risk Analysis

The significance of adequate cyber security protection mechanisms at an urgent care facility cannot be understated. At the very least, the law demands it. Regulations and compliance with HIPAA demand that all healthcare providers, including urgent care providers, follow a basic set of cyber security principles to ensure adequate protection for patient data from threats. The National Institute of Standards and Technology has put forward the HIPAA security rule[3] that aims to assist healthcare providers in understanding the federal information security requirements. These guidelines are intended to facilitate the safeguarding of electronic protected health information (EPHI) which includes the confidentiality, integrity, and availability of this information. This data typically encapsulates medical histories, social security numbers, financial records, etc. Any breach of this data leads to damage of reputation, hefty fines to the provider, and incalculable losses to the

[3] https://www.nist.gov/programs-projects/security-health-information-technology/hipaa-security-rule

patients. It is also possible that business continuity gets affected by a cyber-attack such as ransomware while disrupting critical care for patients. This brief outline cements the significance of conducting a thorough risk and threat analysis for an urgent care center.

3. Painting a Picture of the Threat Landscape

In this section, the authors would like to draw the reader's attention to the landmark study titled "Hospital Resiliency Landscape Analysis" [3]. This study was conducted by the U.S. Department of Health and Human Services, particularly the cybersecurity working group of the HHS. This study[4], in their landscape analysis, aimed to capture the most pernicious dimensions of cybersecurity threats faced by the health care sector in our country. The interesting aspect of this study was that they not only identified the most prevalent threats, but also the methods and techniques used by cyber criminals to disrupt, extort, and compromise the healthcare sector. Using several sound data sets, the working group has identified the following cybersecurity threats as the most numerous:

- Ransomware and Ransomware-as-a-Service (RaaS) attacks
- Cloud related exploitations
- Phishing, Spear-Phishing and social engineering related attacks
- Software and zero—day vulnerabilities
- Denial of service and Distributed Denial of Service attacks (DDos)

The following graphic hopes to capture the diversity and range of attacks and categorizes them into distinct groups.

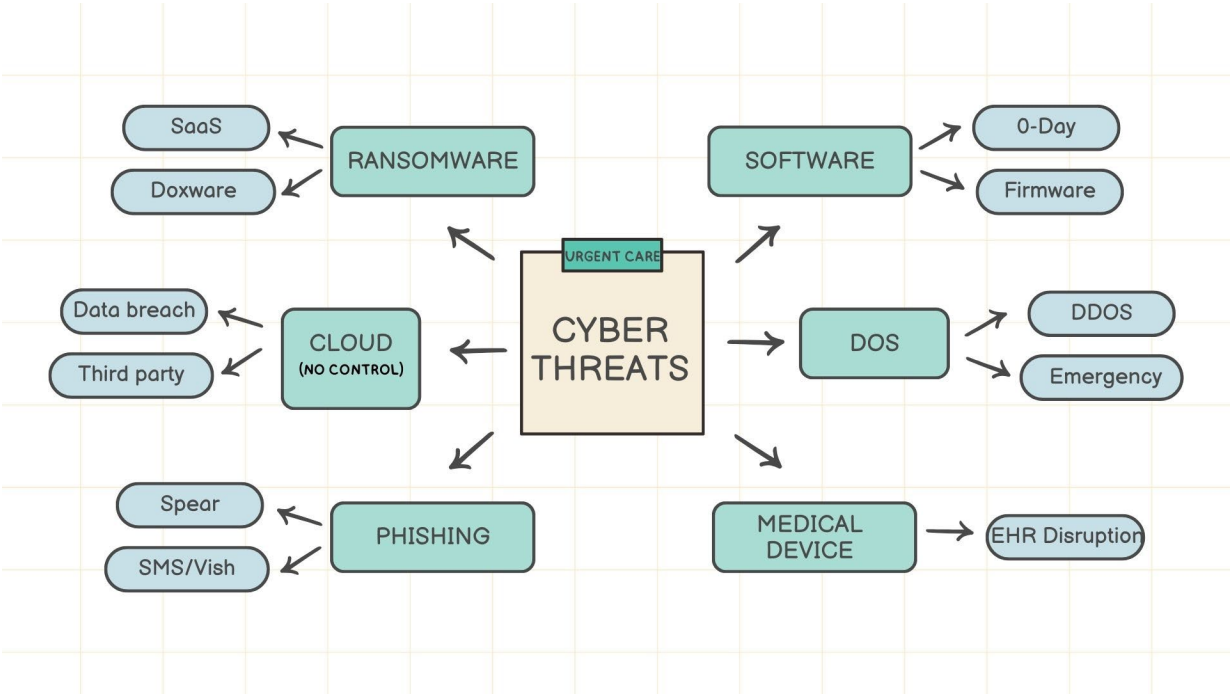

Figure 1: Urgent Care Threat Landscape

[4] https://405d.hhs.gov/landscape-analysis

Let's discuss these threats and risks in some detail below.

a. Cybersecurity Risks

- **Ransomware, Malware, and PII Related Data Breaches**

It is lamentable that urgent care centers typically don't expend as much time, energy, and resources on cybersecurity and information assurance protocols as large hospitals do. Consequently, they often fall prey to malware and related cyber-attacks. Ransomware is a specific type of malware that threatens the victim's access to her data unless a ransom is paid. It is also known as a cryptovirus due to its method of operation. Typically, ransomware encrypts the contents of the victim's hard drive thereby rendering it inaccessible to the victim. It might also threaten to publish sensitive data if the victim refuses to pay up. In the context of an urgent care center, loss of patient data is an unacceptable risk, not to mention the loss of reputation, and revenue. Although, upon payment of the ransom, the decryption key is released to the victim, there are no guarantees that the data will indeed be recovered. This means of attack is therefore also sometimes aptly called cryptoviral extortion. The ransomware itself is delivered to the victim using several channels. The most common channel of delivery is by masquerading the malware as a Trojan horse via an email attachment. Lastly, assuming the urgent care center does pay the ransom, there is no recourse to the fact that the perpetrators now have access to patient data which open up avenues for doxxing. Ransomware attacks are bound to increase in the future merely because of the pervasive availability of RaaS. Ransomware-as-a-service - RaaS - is a model (play on the name SaaS - Software as a Service) where ransomware developers sell their tools and services to other hackers on the cybercriminal marketplace.

- **Cloud and Denial of Service Attacks**

The CrowdStrike annual global threat report (2024)[5] brought to light an increase in 'Access Broker' services. These services focus their efforts on compromising legitimate access to organizations, then selling that access to bad actors looking to commit further objectives, such as ransomware, denial of service, among other attacks. Healthcare is among the top ten sectors advertised by these access brokers. These services facilitate a distributed denial-of-service attack using botnets against an urgent care center by overwhelming the center with traffic, flooding the servers with spurious data and a massive volume of illegitimate requests. Cloud environments, while offering innumerable benefits for a regional urgent care center, do present a unique set of cybersecurity challenges. Chief among these concerns is the fact that tenants have relatively little control over these cloud resources, resources are shared among multiple tenants, and have a complex attack surface. These are some factors that contribute to a greater possibility of data breaches, and denial of service attacks which may lead to emergent medical issues for the patients under the care of these urgent care facilities.

[55] https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf

- **Software, Phishing, and Social Engineering Vectors**

Traditional phishing attacks on most small and medium-sized businesses, including urgent care centers, are launched using email, often scaffolded with social engineering techniques. Because of the reliance on sensitive patient data, urgent care and healthcare facilities are more susceptible to this risk. Some popular variations of the traditional email phishing attacks that are prevalent include 1. SMSishing (using SMS as the carrier vector), 2. Vishing (voice calls), 3. Angler (social media), 4. Clone (creating near-identical copies of legitimate emails), Whaling (targeting high-profile victims, often in the C-Suite), Spear phishing (tailored attacks).

Software vulnerabilities are weaknesses that exist in the operating system, application software, firmware of an IoT device, or other code that can be exploited by the attacker. When an attack exploits a previously unknown vulnerability, it's termed a 0-day (Zero-day) exploit. Buffer overflow, SQL injection, Cross-site-scripting, OS attacks, are some common exploit types. By keeping operational systems patched, and updated routinely, a healthcare facility can mitigate against such vulnerabilities. The interested reader is referred to the NIST Health IT program[6] to learn more about making their organizations more secure.

- **Risks specific to Telehealth, and Medical Devices**

In addition to the risks outlined above which are applicable to telehealth and medical devices, there are some specific, esoteric, risks that afflict this subsector that are worth noting. One big risk with telehealth and medical devices is the risk of misdiagnosis. By design, the health care provider has limited physical examination, and depending on the technical platform, may have difficulties with communicating and/or ascertaining non-verbal cues. Remote data from measuring devices, and/or sensor could lack integrity, and reliance on said impaired data could lead to a false or incorrect diagnosis. Other non-technical sources of risks in this subsector include licensing, policy challenges, geographic/legal disparities, regulatory and compliance issues, and finally equitable access.

b. Physical Security Risks and Issues

While this is not the focus of our research, the challenges faced by most small- and medium-sized businesses are shared by urgent care centers. In some cases, these issues are exacerbated because of the nature of services offered by urgent care centers. Due to the presence of controlled substances, and prescription drugs, expensive medical equipment, urgent care centers are a potential target for theft. The same guidelines that protect any business such as security personnel, lighting systems, locks, surveillance systems, and tight access-control mechanisms, are applicable in this scenario as well. Training staff, and employees on de-escalation along with these other measures can, to some extent, mitigate security issues and create a safer workplace environment for all.

[6] https://www.nist.gov/healthcare

- **Violence in Urgent care Settings**

Not surprisingly, by virtue of the fact that urgent care centers are high-stress work environments, workplace violence related incidents are common. Furthermore, there are patients under pain, under the influence of drugs, or being treated for substance abuse. These factors radically enhance the probability of a violent altercation at an urgent care center. Training staff, and employees on effective de-escalation techniques would be a first step in tackling violence in urgent care workplace environment.

- **Natural Disasters, Disaster Recovery, and Business Continuity, Preparedness**

Natural disasters and emergencies need to be addressed for the successful operation of any business. Certainly, this is of paramount importance for urgent care centers. Disaster recovery and business continuity plans help with being prepared for most contingency scenarios beyond natural disasters and the importance of this cannot be understated. These contingency scenarios include cyber-attacks, active-shooter, fire, earthquakes, hurricanes, flooding, ransomware, insider threats, and other plausible scenarios. Power outages can wreak havoc on a healthcare facility and this unique challenge needs to be addressed from the ground-up and not as an afterthought. Ensuring patient continuity of care under the direst of circumstances is eminently desirable in an urgent care facility.

Generally, the complexity and development of such business continuity plans are handled by experts from a third party. However, having a consultant external to the organization can be an expense that is not justifiable for an urgent care center. Many urgent care centers are migrating towards cloud computing due to its obvious advantages and ease of maintenance. This does come with challenges that has been discussed earlier. Urgent care center proprietors need to have their own data on-premises to eliminate dependency on cloud service providers and need to secure this data. A budget-friendly solution is a deployment scenario that incorporates a backup application running on a local machine that performs duplication of the cloud contents onto local drives. The application interfaces with the cloud on a secure channel, checks for updates and syncs these with the local copy of the data. Some advantages of this methodology include:

- Daily and monthly full backups can be done locally.
- Since storage space in the cloud can be downsized because of local storage, the cost of the cloud storage plan can be reduced.
- Migration from one cloud to another or from public to private or vice versa would be easier since the data is also available locally.

c. Regulatory and Compliance Risks

The healthcare sector faces a constantly evolving regulatory and legal landscape.

- **Ever Changing Legal Frameworks**

Constantly changing laws, particularly surrounding abortions and related controversial care areas need to be traversed delicately by urgent care centers. Stark law prohibits physicians from referring patients to entities where they have a financial interest. For more laws and statutes regarding fraud and privacy, the reader is referred to the portal on the U.S. Department of Health and Human Services, Office of Inspector General[7] that outlines fraud and abuse laws.

- **HIPAA and Data Privacy**

HIPAA, Health Insurance Portability and Accountability Act, demands of health care providers stringent privacy and data protection requirements of their patients' data. The above noted risks are now exacerbated in light of these regulatory requirements. For instance, in addition to the costs imposed by cyber-attacks, data breaches, theft, insider threats, HIPAA violations, including improper use or disclosure of patient data, can also lead to fines and penalties. Urgent care centers can mitigate these issues by implementing robust security measures, and by conducting employee training, in addition to performing routine risk assessments while keeping abreast of changes in laws, regulations and policies.

4. Contributing Factors

Here, let's take a look at some of the factors that contribute to the increase in vulnerability faced by the urgent care centers.

- Greater Attack Surface Area: Increased Dependence on Diverse Technology

  Many health care facilities run the risk of using aging, legacy systems. The allure of upgrading to newer, cloud-based and AI-driven technologies lead many of these urgent care centers to renovate their systems. These systems are complex, interconnected and are bleeding-edge technologies. The vulnerabilities inherent in these systems do not come to light at deployment time but pose a threat during the operational phase of their installation. Using outdated technology or bleeding-edge technology, both have risks inherent to them. Due to the lack of expertise, the knowledge and skills gap, coupled with an increased surface area afforded by the AI-systems all contribute to making an urgent care center all the more vulnerable.

[7] https://oig.hhs.gov/compliance/physician-education/fraud-abuse-laws/

- High Patient Volume and Staff Shortages

  The high-stress environment primarily caused due to the shortage of qualified, and well-equipped staff, and resources leads to fatigue and naturally the probability of falling prey to cyberattacks is radically enhanced. It is well established that social engineering attacks thrive in environments where employee fatigue is pernicious. Also due to the increased patient volume, and the increased demand placed on employees, cybersecurity is often overlooked.

- Increased Frequency of Public Health Emergencies

  It is unfortunate that the reliance on urgent care and emergency room facilities is increasing in the U.S. This problem is only compounded further by the increased frequency of pandemics, attributed by some to increased travel and globalization of our world. There is also a general consensus that infectious microbes and viruses are far more virulent than in the past, leading to the emergence of new, and deadly diseases[8]. Climate change and the concomitant melting of glaciers, and the permafrost have started to release long-dormant, frozen-for-millions-of-years bacteria, viruses, and other microorganisms. These factors, and the associated increase in reliance on urgent care centers, is one of the contributing reasons to making these centers vulnerable.

5. Case Studies

The reader is referred to the seminal document on "Hospital Cyber Resiliency Initiative Landscape Analysis"[9] published by a public-private partnership between Health and Human Services and the Centers for Medicare and Medicaid Services for an in-depth discussion on a few case studies to draw the connection between threats, vulnerabilities, and potential mitigation.

- Incidents reported in Mainstream Media

  While there are unfortunately many stories and reports in the media about cyberattacks on healthcare facilities, in this section, the authors quickly outline a couple to highlight the extent of damage caused by these attacks. The Ryuk ransomware attack[10] on Universal Health Services (UHS) caused a huge financial loss. While UHS isn't a small urgent care center, his example is used to highlight the losses that can potentially be faced by an organization due to a cyberattack. The losses sustained by Scripps Health were far greater than that of UHS[11]. In addition to

[8] https://pmc.ncbi.nlm.nih.gov/articles/PMC10673331/
[9] https://405d.hhs.gov/Documents/405d-hospital-resiliency-analysis.pdf
[10] https://www.hipaajournal.com/scripps-health-ransomware-attack-cost-113-million/
[11] https://www.fiercehealthcare.com/health-tech/scripps-ransomware-post-mortem-shows-cybersecurity-regional-problem

the ripple effects that the Scripps attack had on neighboring hospitals, Scripps Health was also made to pay millions of dollars to patients affected by the data breach[12]. The case studies listed thus far were of large hospital systems. Let us know, finally, as a cautionary tale discuss the nightmare faced by a two-doctor ENT and Hearing services health care facility[13]. A ransomware attack erased all the records which led to the doctor's office closing down. This may have been the first-known case of a doctor's office going out of business due to a ransomware attack.

- Important takeaways
  This goes to show that businesses, large and small, in the healthcare sector are exposed to this risk and suffer the consequences alike. Larger hospital systems may be better equipped to deal with such threats, smaller providers, including urgent care centers may be left with no choice but to shutter their doors because of a cyberattack.

6. Risk Mitigation Strategies

This section briefly outlines the risk mitigation strategies used by most corporations and considers how one might apply these techniques in the context of urgent care facilities. This discussion includes options to avoid, reduce, accept, and transfer risk.

- Cybersecurity Hardening Measures

  Measures such as data encryption, network security and vulnerability analysis, security audits, and routine penetration testing can reduce the risk exposure of an urgent care facility. Coupled with strong access control mechanisms, including multi-factor authentication systems (biometrics, tokens, passwords), password management policies, employing the principle of least privilege (granting a user the lowest level of access to the system to perform their task), are some options to harden an organization's security posture. These are steps one could take to reduce risk.

- Enhancing Security Protocols

  Security protocols, both in the physical and cyberspace domains, need to be constantly updated and managed. Ongoing maintenance and improvement of these protocols are paramount to the smooth operation of the facility. Evaluating if these protocols meet the needs of the stakeholders while balancing usability and security is important. Seeking expert advice is advisable since this is a constantly evolving arena. This includes updates and patches of all computing devices used at the facility. Software patches, and firmware upgrades as needed, followed by protocol

[12] https://www.cbs8.com/article/news/local/scripps-health-pay-3-million-to-patients-ransomware-attack-2021/509-5d14c0f0-cbae-413e-b715-f68ef56002a1
[13] https://www.startribune.com/all-of-records-erased-doctor-s-office-closes-after-ransomware-attack/508180992

upgrades for telehealth and other network tools used at the establishment. Limiting use of outdated technology can avoid risk.

- Training and Crisis Management for stakeholders

  Health care providers could train their employees, minimize staff with access to sensitive data, to manage risk. Of course, insurance serves as the primary mechanism with which to transfer risk. Lastly, some measure of risk must necessarily be absorbed and accepted into the daily operation of a health care facility as the routine cost of running a small to medium-sized healthcare business.

7. What Does the Future Hold

We live in an interesting time – each day, all of us perceive the inexorable march of technology and its impact on our lives. This omnipresent force of technology has an outsized influence on the future of healthcare. Let's investigate this briefly in this section.

- Emerging Technologies and Their Implications

  No discussion of emerging technology can omit a mention of AI (Artificial Intelligence), machine learning, and data analysis. There are great advances being made in healthcare, thanks to these tools and technologies. Some notable mentions include personalized medicine, gene editing capabilities and gene therapy, robotics (surgery and precision tools), IoT (telehealth applications and smart hospitals), Block-Chain and related technologies have enhanced security systems while minimizing operational burden. Patient engagement, and education has come a long way with the advent of augmented and virtual reality (AR and VR). Some challenges that society has begun to encounter with these strides in technology include privacy and security concerns. This report has discussed in the previous sections some of the consequences associated with loss of confidentiality and integrity. These new and advanced tools, in the hands of cyber attackers, pose a serious threat to the entire framework of healthcare. Others concerns in the age of emerging technologies are those pertaining to ethics and morality. These are primarily around the issues of gene editing and related therapeutic solutions. As technologies evolve, so does the need for regulatory and policy landscape that governs them. The burden of keeping up with these laws and policies fall on the shoulders of the urgent care proprietor.

- Anticipated Threat Evolution

  In terms of predicting the optimal strategy for the future in light of these advances in technology, it is our firm belief that transparency and collaboration among the diverse stakeholders is the key. Being forthright and clear with patients about how data will be used would be a necessary first step in this direction. Rather than embrace every bleeding-edge technological innovation, an urgent care center should prioritize patient autonomy and care and only embrace those tools that serve this primary goal. Collaboration among the key parties – patients, medical professionals, policy

makers, and researchers to ensure that this overarching goal is met is essential. Patients need to be empowered and be offered greater power and agency in their care and on the use of their data. This, in our opinion, would be the best approach to evolve in harmony with these emerging technologies and the most effective way to be the most generative with it so as to have a salutary effect on the health of the patients.

8. Conclusion

This report has attempted to inspire urgent care centers in Texas and around the country to be mindful of the rapidly evolving landscape of cyber threats and attacks. The report has brought to bear the best forecast and predictions on the nature of cyber threats facing urgent care centers in the next decade using reports from a diverse set of sources. Lastly, being proactive, our report will hopefully serve as a guide to be prepared and protected against some of these projected trends in threats and attacks for the next decade.

9. Acknowledgement

The authors would like to thank the support and funding from *The Institute for Homeland Security* (IHS) at Sam Houston State University, Huntsville, TX. The Institute aims to provide innovative, value-added knowledge to protect critical infrastructure and support commerce, tailored to the needs of industry and government. The Institute is a center for strategic thought with the goal of contributing to the security, resilience and business continuity of these sectors from a Texas Homeland Security perspective.

10. Additional Resources and References

1. Miller, W. L. (2021). The story of general practice and primary medical care transformation in the United States since 1981. Commissioned paper for the NASEM Consensus Report: Implementing high-quality primary care rebuilding the foundation of health care, 1-60.
2. Hoffer, E. P. (2024). Primary Care in the United States: Past, Present and Future. The American Journal of Medicine.
3. Decker, E., Wood, R., Mohiuddin, S., Nock, D., & Venugopalan, A. (2023). Hospital Cyber Resiliency Initiative Landscape Analysis. HHS 405 (d).

INSTITUTE FOR HOMELAND SECURITY

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Water / Wastewater, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security
Sam Houston State University

Shashidhar N., & Varol, C. (2025). Emerging Threats Against Urgent Care Centers (Institute for Homeland Security Report No. 2025-1003). Institute for Homeland Security.
https://doi.org/10.17605/OSF.IO/Y9CKX