Ontological Security and Threat Mitigation in Healthcare: A Descriptive Exploration

Brandon Griffin[1], Michaela Barnett[2], Tom VanNorman[3], Nina Janine Medina[3], Lucas Potter[4] and Xavier Palmer[4]

[1]Cyberlinc, USA
[2]Blacks In Cybersecurity Headquarters, Inc., USA
[3]Biohacking Village, USA
[4]BIOSView Labs, USA

bgrif023@gmail.com
michaela@bichq.org

Abstract: The healthcare sector's growing reliance on interconnected cyber-physical systems, from electronic health records (EHRs) to networked medical devices, has expanded both operational capabilities and systemic vulnerabilities. The costs associated with cyber-attacks have become a financial burden for the global healthcare sector, with estimates whose substance is capable of bankrupting institutions. These costs underscore the urgent need to analyze expanding attack surfaces at the intersection of cybersecurity and biosecurity [cyberbiosecurity (CBS)/biocybersecurity (BCS)], requiring systematic identification of targetable assets and corresponding defense protocols. This paper analyzes healthcare's evolving threat landscape through the lens of ontological security. The commentary focuses specifically on threats to living systems and biological data integrity (e.g., genetic, biometric), suggesting how a focus on these unique biological targets necessitates a shift from purely IT-centric defense to a human-centric risk posture. Addressing this, we draw on the synthetic definition of ontological security which addresses stability from continuity of experience in one's life and apply it to the healthcare space. From here, we build on the notion of perceptions of secure healthcare spaces aiding care received, we attempt to spotlight potential consequences relating to vulnerabilities in healthcare that could link to lapses in patient care, including identity fragmentation during biometric theft, temporal collapse from ransomware-induced care delays, and spatial destabilization via telemedicine breaches. The paper provides a commentary that draws on select literature, drawing on a combination of techniques and observations that can restore lapses in ontological security. We address ethical imperatives for protecting biometric and genetic data, as central targets in this expanded threat landscape, while outlining policy measures to future-proof healthcare systems against AI-driven threats. By centering existential safety alongside technical safeguards, this work redefines healthcare cybersecurity as a covenant of human security in an increasingly digitized care ecosystem. The goal of this exploration is to provide global health institutions with considerations to aid care strategies that simultaneously protect patient safety, provider integrity, and institutional resilience.

Keywords: Ontological security, Cybersecurity, Biocybersecurity, Cyberbiosecurity, Attack surfaces, Healthcare

1. Introduction

Attacks on healthcare are part of the "new normal" within cybersecurity, and failure to account for the consequences of actors exploiting these attack surfaces, especially with advanced technologies, can yield severe consequences (Razaque et al, 2019; Dimitrov, 2020; Fouad, 2024). Modern healthcare operates within an increasingly interconnected cyber-physical ecosystem where critical infrastructure, including electronic health records (EHRs) systems, networked medical devices and telemedicine platforms converge to enhance patient care. However, this digitization expands the attack surface for malicious actors, introducing unprecedented risk to data integrity, service continuity and ontological security. "Attack surfaces" (Theisen et al, 2018) as a term encompasses numerous definitions surrounding the context and purposes of this paper. We refer to numerous cyber-physical environments and surfaces that can be exploited to be the target of an attack. Ontological security is the foundational sense of safety and trust to be used in this context to refer to a Cybersecurity disposition (Griffin et al., 2023). Cyber-physical attacks have the chance to upend a sense of safety and trust, particularly within the delicate subject matter of patient care. Healthcare institutions represent target-rich environments for cyber-physical threats (Al;-Qarni, 2023; Li et al, 2025). Technical vulnerabilities in medical devices such as ventilators, pacemakers, patient monitors or infusion pumps can combine with human factors and interaction from activity such as social engineering, phishing or baiting. Additionally, supply chain weaknesses create exploitable entry points; these threats extend beyond operational disruptions to directly compromise patient ontological security. Breakdowns in institutional reliability during ransomware-induced care delays are the latest, with a notable example being the WannaCry attack (Collier, 2017). The COVID-19 pandemic significantly exacerbated these vulnerabilities by accelerating telemedicine adoption in an uncertain time (Alanazi, 2023). Additionally, inclusion of cloud computing and

adjacent technology has presented numerous attack surfaces to protect and evaluate (Kubendiran et al, 2015; Zhang et al, 2015; Van Devender et al, 2023).

This paper analyzes healthcare's attack surfaces through the lens of ontological security, examining mainly identifiable interconnected target groups; technical systems, operational technology (OT), information technology (IT), human targets, and systemic structures, among others. Initially, technical systems where compromise enables life-threatening manipulation of devices or theft of immutable biometric data. Further, human targets including clinicians, patients and supporting staff where coerced actions or eroded agency undermine relational trust. Additionally, systemic structures such as supply chains and access control where failures disrupt the environmental stability essential to ontological safety. Without enforceable standards and cross-sector collaboration, these vulnerabilities risk institutionalizing ontological insecurity. This manifests through care avoidance, clinician burnout, and general distrust (Vukotich, 2023). Effective mitigation requires socio-technical strategies addressing both cyber-physical risks and their existential repercussions. In addition to creating a framework, this work aims to open up additional considerations of security focused on BCS/CBS in the healthcare context and invite further research from adjacent communities.

2. Themes Explored

This paper offers a synthesis of healthcare infrastructure with themes or cases for analysis. Vulnerabilities across core concepts draw on a curated selection of relevant literature published between 2006 and 2024. These concepts are Cyber-physical Systems (CPS), Attack Surfaces and Vulnerabilities, Biocybersecurity (BCS) / Cyberbiosecurity (CBS), Ontological Security, Identity, Risk and Workforce Preparedness. These are thematically structured for this discussion. Pertinent literature regarding supportive frameworks was included as applicable. The selection was informed by multiple, non-systematic search sessions in relevant databases using a broad range of key terms, including, but not limited to: "cyber-physical systems," "healthcare," "cybersecurity," "Internet of Medical Things," "attack surface," "cyberbiosecurity," "biocybersecurity," "health," "biotechnology," "workforce," "defense," "ontological security," "cyber," "biotechnology," "nation-state," and "bio-economy." This commentary does not follow a systematic review methodology; rather, it acts as a commentary that highlights some important developments and connections across these fields to frame the ongoing discussion on security. BCS and CBS serve as a foundation for this commentary, having been covered extensively in prior work (Potter et al, 2021; Potter and Palmer, 2023; Greenbaum, 2023). These terms involve phenomena that have interplay between biosecurity, cyber-physical security, and cybersecurity contexts within the bioeconomy. The following sections are distillation of insights based off of such papers. These do not represent final or total thoughts on the intersections discussed but merely an opener. What is essential to note is that healthcare is not merely a technological process but one that is at the intersection of social processes, organizational dynamics, infrastructure and diverse perceptions.

3. Healthcare Attack Surfaces

Healthcare systems face a complex and overlapping set of attack surfaces that make them prime targets for cyber threats. Figure 1 gives a simple map of processes that can be made a target of. These vulnerabilities span technical, human, systemic dimensions and/or a hybrid, with each introducing unique risks to operational continuity, data integrity and ontological security.

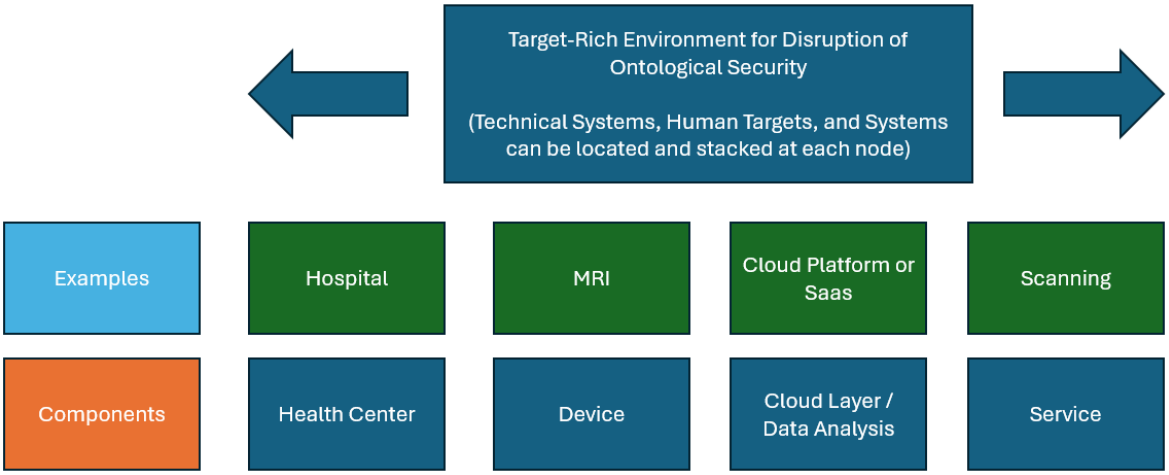

Figure 1: Map of targets within a Healthcare attack surface. Attacks can be stacked along the axes of the number of vulnerabilities and components for combinatory effects

Technical attack surfaces include devices, networks, and software, providing numerous entry points for malicious actors to exploit or disable critical systems. Examples range from networked medical devices like patient monitors, infusion pumps, or imaging modalities [Magnetic Resonance (MR), Medical Extended Reality (XR), and Computed Tomography (CT)] to electronic health record (EHR) platforms and hospital network infrastructure.

It helps planners to conceptualize the components that can be accessed by malicious elements (Spanakis et al 2020; Verma, 2022). These systems can be compromised due to device and institutional misconfigurations, weak cyber hygiene, or outdated software, and while they may not always be primary targets, their role in storing or accessing sensitive data makes them attractive secondary assets for attackers (Wasserman and Wasserman, 2022; Rajora et al, 2022; Aloufi et al, 2025). Medical devices can act as repositories for sensitive data, their role in storing patient safety information makes these a significant technical target (Mirsky, et al., 2019). Along with this, challenges and unique circumstances in asset identification and vulnerability assessment further complicate the attack surface and landscape (Skorobogatjko et al, 2014; Sultanovs et al, 2016; Van Devender & Mcdonald, 2023).

Human elements in threat modelling are often identified as involving next-of-kin, patients, staff, personnel and contractors. All of which listed are vulnerable to social engineering methods that may coerce action or initiate a malicious action. Healthcare professionals are frequently targeted due to their access to sensitive patient data and critical systems (Alavi et al., 2024; Gilbert et al, 2024). Employees such as administrative or maintenance staff, may also be exploited through financial incentives or limited cybersecurity training, providing attackers with physical or digital access to restricted areas. Their access to server rooms, storage closets, restricted areas, or personnel areas provide an advantage (Muthuppalaniappen & Stevenson, 2020). Patients and visitors represent additional targets as their personal devices and trust in healthcare environments can be manipulated to gain broader network access in various emotional, mental, or physical states or varying pain and distress levels.

Attack surfaces regarding interconnected systems, defined as “systematic” in this discussion, encompass supply chain weaknesses and auxiliary infrastructure vulnerabilities. Third-party vendors, outsourced IT services, and medical suppliers often operate with inconsistent security standards. This creates hidden entry points for attackers. Technical compromises can lead to life-threatening situations, such as manipulated medical devices or ransomware-induced treatment delays. Human-centered attacks erode trust and enable broader network breaches; while systemic vulnerabilities disrupt essential services and supply chains. In this discussion it is a focal point to highlight ransomware attacks as they can halt pharmaceutical, payment or record systems. Overlapping attack surfaces highlight the need for comprehensive, layered security measures that address not only technical flaws but also human behaviors and systemic weaknesses in this uniquely sensitive environment centered around very human factors that depend on technical systems. Protecting these domains is essential for safeguarding both operational functionality and the ontological security of patients and providers. Auxiliary systems, including HVAC controls, facility access systems, supply chain logistics, and point of sale (POS) devices, are frequently overlooked in security planning despite their critical

roles in hospital operations (Millett et al, 2019; Neprash et al 2022; Al-Qarni, 2023; Li et al, 2024; Li et al, 2025; Park and Lim, 2025). For example, HVAC tampering can compromise climate-sensitive medications or equipment, while POS breaches can expose financial data and disrupt billing processes. These systems are particularly vulnerable when they are not properly segmented from core clinical networks or when security configurations lapse due to perceived low priority (Muthuppalaniappen & Stevenson, 2020).

Patients and providers need not fall to the conceit that malicious actors will not stack newly developed technologies to amplify their interference and planned disruption. For example, artificial intelligence can be used to amplify quality and quantity of attacks, to improve the odds of successful breaches and or disruption (AlZubi et al, 2021; Bonagiri et al, 2024). The discussion of AI agents and its involvement in supporting threat actors has been a point of contention (AlZubi et al, 2021; Bonagiri et al, 2024; Qiu et al, 2024; Jumaah et al, 2025). Generative AI applied to conversations and records without consent can result in a vector for exploration. Healthcare systems and insurance companies, regardless of who owns them, are at risk depending on the scale of attacks that occur at this intersection (Yeo and Banfield, 2022; Brilhante et al, 2025). Further, elements sustaining such as conceptualized in Figure 1, draw important salient points on how ontological security can be meaningfully degraded.

4. Ontological Security Concerns and Implications

The concept of ontological security refers to a state where an individual perceives their existence as authentic, intact, protected, and secure from the external factors in everyday life. In the context of healthcare, ontological security manifests as patient and provider confidence in the reliability and safety of medical care systems and environments (Griffin et al., 2023). Cyber-physical attacks on healthcare infrastructure directly undermine this fundamental sense of safety, generating profound implications for individual wellbeing and institutional trust.

Technical vulnerabilities precipitate ontological insecurity with their impact. This includes violating bodily autonomy, privacy, and personal identity. Compromised medical devices can transform therapeutic tools into sources of threat; with potential of eroding patient trust in their own bodies, treatment protocol, prescriptions, and the medical system as a whole. Biometric data theft further destabilizes identity integrity, as stolen genetic or physiological information represents an immutable personal exposure. Such violations transcend financial or privacy harms, striking at the core of an individual's perceived safety in medical care at their most vulnerable moments. Home, Holistic or Alternative Care should be discussed here as it belongs to the hemisphere of this subject matter, however, due to homeopathic belief systems it has departed from this ecosystem. While not directly intertwined with the hospital healthcare infrastructure, digital technologies are widely integrated into modern societal life. The common use of mobile applications, website archives, digital health platforms, and virtual support communities are worth noting as they may be used to inform or derive actions in members of this healthcare community. This can serve as a unique target or point of influence.

In home environments personal devices such as “smart” or integrated personal first aid devices, OTG scopes, cameras, and allocated monitors can deliver meaningful value in interaction with healthcare personnel as patients seek to gather knowledge to share or self-diagnose. However, these at-home care products with a goal for intended domestic use can differ considerably more in function and quality than hospital grade devices in terms of manufacture, security considerations, and components. While this portion of subject matter is listed as a point of reference, the topic has the depth and breadth to facilitate a separate discussion. (Dey et al, 2018; Ghirardello et al, 2018; Plappert et al, 2021; Parsons et al, 2023).

Human-centered attacks amplify relational and institutional distrust through a variety of mechanisms. Social engineering campaigns targeting clinicians corrode professional autonomy and introduce moral injury when individuals become the conduit for a breach of security. Patients subjected to coercion or manipulation experience eroded sense of self-reliance in decision making or personal authority, while broader institutional breaches foster collective uncertainty. Healthcare workers in turn can experience increased stress related to post-event scrutiny, leading to burnout and job dissatisfaction (Alanazi, 2023). To illustrate this, by examining the effects of pandemics, the misinformation distributed and the general consensus it can be observed that these effects significantly intensified (Muthuppalaniappan & Stevenson, 2020; Dixon, 2023). These periods of time as of late tend to generate an environment for accelerated digital transformation while sustaining weakened support structures or analysis.

Systemic disruptions, overall, create environmental and temporal instability that further undermine ontological security. For examination, supply chain attacks such as those targeting blood product deliveries

sabotage the predictable infrastructure necessary for continuous care (Vukotich, 2023). Ransomware-induced service delays fracture expectations of treatment, creating uncertainty about future care availability and integrity (Alanazi, 2023). Even auxiliary system compromises transform clinical environments to extensions of a landscape containing a potential threat. Factors of this scenario affect both patient care and medical supply integrity. Medical device manufacturers have responsibilities centered around the duty to warn. In the medical device industry, manufacturers are often considered to have fulfilled their obligation to warn end users (patients) by providing adequate warnings and instructions to the formally educated intermediaries (medical professionals and the adjacent) who administer these devices. The rationale utilized to validate this stance conveys that healthcare professionals are “better positioned” to understand the complexities of a manufacturer's medical devices and potential risks (Bown, 2017). The professionals slated to communicate these effectively to the patients based on individual cases are thus implied to be the "responsible" party.

Implications discussed here necessitate redefining healthcare cybersecurity beyond technical compliance. Protecting ontological security requires frameworks that address these niche threats, ensuring that encompassing defense strategies safeguard not only data and devices, but also those the system seeks to support. This approach recognizes that maintaining ontological security is essential for ensuring patient confidence and supporting healthcare providers in delivering service (Steele, 2008).

5. Cyber-Physical Risk Mitigation Considerations

Healthcare is the ultimate critical infrastructure. Securing IT systems and infrastructure within Healthcare and related Biomanufacturing, are the cornerstones of maintaining best practices and improving security posture.

Healthcare organizations face a wide range of cyber threats. These threats have the capability to disrupt patient care, steal, or alter sensitive data such as PII, PHI, financial information, or disrupt critical infrastructure that organizations need to safely operate. An example of critical infrastructure systems in organizations are in Building Management Systems (BMS) that control clean room pressures, heating and cooling systems, lighting, power and water purification systems.

Conceptually, the latest addition to the factors listed is the Internet of Biological Things (IoBT) has been discussed among scientific practitioner communities, and it is recommended that this community develops secure-by-design principles for the IoBT before the underpinning biotechnologies are incorporated in mass.

Effective Healthcare Operational Technology (OT) cybersecurity relies on defense in depth. This approach combines people, processes, and technology. Core practices include ICS-specific incident response planning, network segmentation, secure remote access, risk-based vulnerability management, and continuous monitoring. Standard IT practices also apply, such as patching, strong credentials, and embedding security into procurement. However, OT patches must be tested in isolated environments before deployment to avoid operational disruptions or malicious updates.

Effective defense of healthcare environments requires integrated mitigation frameworks that address technical, human, and systemic vulnerabilities, as discussed. These frameworks must extend beyond conventional Cybersecurity to incorporate sociotechnical principles and ontological safety objectives. These must align with Healthcare IT Security with general governance as there is work toward enhancing trust (Ewoh & Vartiainen, 2024). A multi-layered approach is essential to protect both operational functionality and the foundations of care delivery.

Technical mitigation begins with architectural resilience. Zero-trust security models, which assume no implicit trust for any user or device, provide a foundational strategy for protecting networked medical devices and electronic health records (Patel et al, 2023). Network segmentation and strict access control, isolate critical clinical systems from auxiliary infrastructure such as Building Automation Systems (BAS) e.g.; HVAC, payment systems, and adjacent support dashboards. This containment limits lateral movement by attackers, a key recommendation for protecting auxiliary systems (Muthuppalaniappen & Stevenson, 2020). Regular vulnerability assessments and patch management protocols are necessary to address weaknesses in medical device software and hospital operating systems. As this subject matter advances, AI powered solutions are becoming a more common proposition for anomaly detection or AI-driven threat hunting, with a goal to enable proactive identification of issues before they disrupt clinical operations.

OT environments have overlapping technologies with IT systems. However, the priorities and purpose of each system are very different. OT environments focus on availability and safety, where IT systems typically focus on confidentiality while addressing integrity and availability. OT systems are designed to operate for ten to

fifteen years or longer which can lead to unsupported technology without existing support, legacy systems in this case cannot easily be replaced without pairing a successor, large expense, and coordination. Developing a strong OT security program includes coordinated policies, training, and clearly defined roles. Ongoing auditing will ensure both the cybersecurity of OT systems and the physical system remains in a reliable operational state geared toward servicing patient care. Figure 2 provides examples of attacks to Healthcare OT Systems.

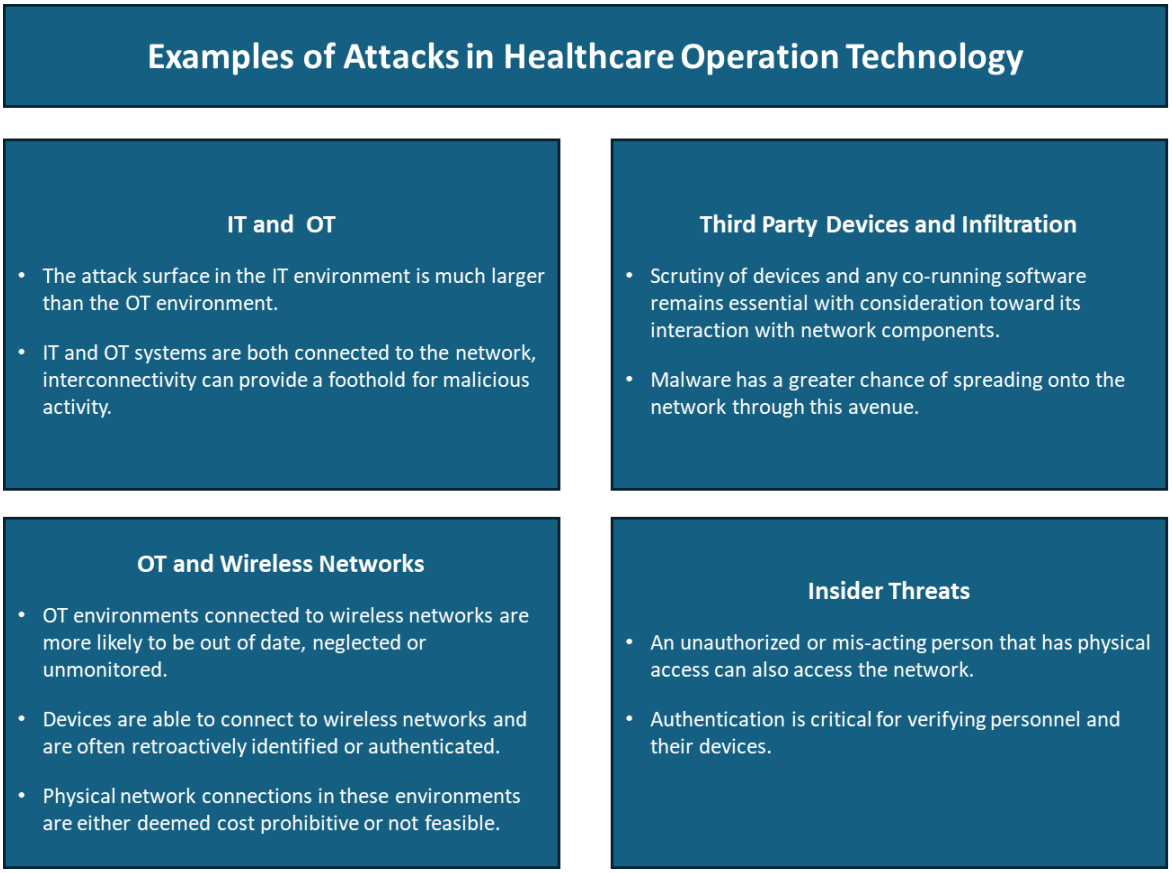

Figure 2: Examples of Attacks to Healthcare Operational Technology (OT) Systems. Attacks and misconfiguration can cause operational disruption or avenues for malicious activity

6. Discussion: Long-Term and Ethical Considerations

When we reflect on the concept of "do no harm" there exists importance in forward adjusting how we reasonably reduce harm for patients through ensuring safety. Ethics will be condensed around how urgency is a factor towards promoting better ontological security for patients and providers. Technological advancements continue to be introduced to patients, providers and hospitals and have been reactive to cybersecurity components and practices, including "Shadow IT". IT systems and components not approved officially by IT, as a supplement to approved systems define Shadow IT (Silic and Back, 2014; Raković et al, 2020; Patel et al, 2023).

There exists continuing value in assessing how actors may present unauthorized threats to existing infrastructure and how countermeasures may need to evolve over time. For example, health security research from the recent past demonstrates the ability of actors to introduce malicious hardware/software or bypass internal systems to deploy damaging or extractive action as more plausible especially, with the addition of human interaction and physical security elements (Mirsky et al, 2019; Wasserman and Wasserman, 2022; Marti, 2025).

Those masquerading as active patients, next-of-kin, personnel, or visitors can easily record conversations, as a scenario for examination, where sensitive information can be captured and utilized to manipulate individuals or systems. Actors may be able to engage with abandoned computers, as physicians and staff are distracted or not present. Consumer level and concealable tools that can clone electronic assets from a close proximity or infiltrate devices through malicious cables allow actors to gather data and execute hardware-based attacks.

Malicious software introduced into hospital workflows can be designed to rapidly learn and adapt to countermeasures to evade detection for longer, learn more about their host architecture or grow more potent. These are examples of the ability for actors to integrate into the fast paced and rapidly evolving care environment where healthcare workers practice and serve, often in cadence with one another.

Additionally, acquisitions of medical institutions by larger firms guided by an opportunity for financial gain or a business decision, versus a client focused or intentional accumulation, can pose a risk. Often the aim is to manage facilities and their operations at minimal cost. This exacerbates the vulnerability in maintaining medical infrastructure in its entirety including managing and staffing. In this environment, security is not prioritized. Access to a facility, access-controlled areas, PII or credentials can be easily acquired through abusing poorly executed practices or misinformed and undertrained personnel.

Threats like these, stand to be amplified as more technological integration continues and arguably already are. Scenarios discussed here highlight conditions of failure in ontological integrity. Reduced patient patronage as well as increased distrust of providers (and their institutions) can have a cascading effect on the degradation of applied healthcare. Solutions include what can be derived from practices that emphasize bolstering security measures and maintaining a transparent dialogue about emerging threats.

7. Limitations and Future Work

This work is a commentary, collecting considerations across a mix of works that also include conference proceedings and non-peer reviewed work. It takes on more of a conceptual nature and does not claim quantified analysis. Future work may involve further focused analytical work on ontological cyberbiosecurity perceptions focused in healthcare.

8. Conclusion

This paper explores how the increasing digitization of healthcare, from electronic health records to networked medical devices, creates a unique environment for vulnerabilities that undermine ontological security. The foundational sense of existential safety and trust for patients and providers is at the primary emphasis. Utilizing insights from prior works explored, this paper categorizes these attack surfaces into technical, human, and systemic domains. This outline serves as a canvas, detailing how compromises can lead to issues like identity fragmentation, care delays, and relational distrust. Research highlights the profound consequences of these vulnerabilities, including increased patient care avoidance and clinician burnout. The authors propose a socio-technical mitigation framework that combines zero-trust architectures, staff training, and cross-sector collaboration to reinforce ontological security. Cybersecurity considerations in the Healthcare environment are a commitment to human safety in a digitized world, aiming to provide a framework for global health institutions to protect patient safety, instil provider integrity and support institutional resilience.

Acknowledgements

Special thoughts of appreciation go out to/among staff within Hospitals, Medical Device Manufacturers and Technicians, Those of the Hacker Community Devoted to Curiosity, Improvement, and Collaboration. Additional acknowledgements go out to Ron Stephenson, Dr. Srdjan Lesaja, C.B, C.W, I.M., J.W., J.P., K.S., M.H., and others who contributed to an alternative iteration of this work.

Ethics Declaration: Ethical clearance for the research referred to in this paper was not required as no experiments were conducted.

AI Declaration: Google Docs tools were used to organize writing within this manuscript.

References

Adeoye, S.O., Lindberg, H., Bagby, B., Brown, A.M., Batarseh, F.A. and Kaufman, E.K., 2023. Cyberbiosecurity Workforce Preparation: Education at the Convergence of Cybersecurity and Biosecurity. *NACTA Journal*, 67, pp.341-351.

Alavi, A., Anvari, S., Isautier, J. M. J., & Seoudi, N. (2024). The cybersecurity landscape of telemedicine: Threats and solutions. *npj Digital Medicine*, 7(1), 44.

Aloufi, R.A.M., Alsuhaymi, N.K.N., Almutairi, A.M.M., Aljohani, M.D.D., Altarjami, R.D.D., Alharbi, A.A.S., Alrehaili, R.A.N., Alraddadi, A.E.A., Alrehaili, R.A.N., Alraddadi, S.E.A. and Alruwaythi, T.B.M., 2025. Cybersecurity and Physical Security Integration in Healthcare Institutions: Protecting Data, Infrastructure, and Human Lives. *Cultura: International Journal of Philosophy of Culture and Axiology*, 22(5s), pp.45-51.

Al-Qarni, E.A., 2023. Cybersecurity in healthcare: A review of recent attacks and mitigation strategies. *International Journal of Advanced Computer Science and Applications*, 14(5).

AlZubi, A. A., Al-Maitah, M., & Alarifi, A. (2021). Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques. *Soft Computing*, 25(18), 12319-12332.

Bonagiri, K., VS, N.M., Gopalsamy, M. and SJ, S., 2024, August. AI-driven healthcare cyber-security: protecting patient data and medical devices. In: *2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI)*. IEEE, pp. 107-112.

Brilhante, M.F., Mendonça, S., Pestana, P., Rocha, M.L. and Santos, R., 2025. Economic impact of healthcare cyber risks. *Health and Technology*, 15(3), pp.635-650.

Collier, R., 2017. NHS ransomware attack spreads worldwide. *Canadian Medical Association Journal*, 189(22), pp.E786–E787. doi:10.1503/cmaj.1095434. Available at: https://pmc.ncbi.nlm.nih.gov/articles/PMC5461132/ (Accessed: [insert date]).

Dey, N., Ashour, A. S., Shi, F., Fong, S. J., & Tavares, J. M. R. (2018). Medical cyber-physical systems: A survey. *Journal of medical systems*, 42, 1-13.

Dimitrov, W. (2020). The impact of the advanced technologies over the cyber attacks surface. In: *Artificial Intelligence and Bioinspired Computational Methods: Proceedings of the 9th Computer Science On-line Conference 2020, Vol. 2 9*. Springer International Publishing, pp. 509-518.

Dixon, T.A., 2023. The bioinformational dilemma: where bioinformational diplomacy meets cyberbiosecurity. *Australian Journal of International Affairs*, 77(2), pp.169-187.

Fouad, N.S., 2024. Cyberbiosecurity in the new normal: Cyberbio risks, pre-emptive security, and the global governance of bioinformation. *European Journal of International Security*, 9(4), pp.553-573.

Ghirardello, K., Maple, C., Ng, D., & Kearney, P. (2018, March). Cyber security of smart homes: Development of a reference architecture for attack surface analysis. In: *Living in the Internet of Things: Cybersecurity of the IoT-2018*. IET, pp. 1-10.

Gilbert, S., Ricciardi, F., Mehrali, T. and Patsakis, C., 2024. Can we learn from an imagined ransomware attack on a hospital at home platform?. *NPJ Digital Medicine*, 7(1), p.65.

Greenbaum, D. ed., 2023. *Cyberbiosecurity: A new field to deal with emerging threats*. Springer Nature.

Griffin, B., Alexander, K., Palmer, X.-L. and Potter, L., 2023. Social-Engineering, Bio-economies, and Nation-State Ontological Security: A Commentary. In: *Proceedings of the 18th International Conference on Cyber Warfare and Security*, 18(1), pp.111–118. doi:10.34190/iccws.18.1.1021.

Jumaah, M., Yassin, A.A., Abduljabbar, Z.A., Jawad, M. and Nyangaresi, V.O., 2025, April. Malware Detection in a Healthcare System via Artificial Intelligence Technology: A Review. In: *Computer Science On-line Conference*. Cham: Springer Nature Switzerland, pp. 90-113.

Kubendiran, M. & Murugaiyan, A. (2015). Ontology based Access Control Model for Healthcare System in Cloud Computing. *Indian Journal of Science and Technology*, 8, 218. 10.17485/ijst/2015/v8iS9/53617.

Li, C., Wang, J., Wang, S. and Zhang, Y., 2024. A review of IoT applications in healthcare. *Neurocomputing*, 565, p.127017.

Li, S., Surineni, K. and Prabhakaran, N., 2025. Cyber-Attacks on Hospital Systems: A Narrative Review. *The American Journal of Geriatric Psychiatry: Open Science, Education, and Practice*.

Marti, C., 2025. May 30th, 2025 Competition and Cybercrime: A Theoretical Assessment and Empirical Application.

Millett, K., Dos Santos, E. and Millett, P.D., 2019. Cyber-biosecurity risk perceptions in the biotech sector. *Frontiers in bioengineering and biotechnology*, 7, p.136.

Mirsky, Y., Mahler, T., Shelef, I. and Elovici, Y., 2019. {CT-GAN}: Malicious tampering of 3d medical imagery using deep learning. In: *28th USENIX Security Symposium (USENIX Security 19)*, pp. 461-478.

Muthuppalaniappan, M., & Stevenson, K. (2020). Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to global health. *Journal of Medical Internet Research*, 22(8), e23410.

Neprash, H.T., McGlave, C.C., Cross, D.A., Virnig, B.A., Puskarich, M.A., Huling, J.D., Rozenshtein, A.Z. and Nikpay, S.S., 2022, December. Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016-2021. In: *JAMA Health Forum*, 3(12), pp. e224873-e224873. American Medical Association.

Park, E. and Lim, J.H., 2025. The impact of healthcare data breaches on patient hospital visit behavior. *International Journal of Research in Marketing*.

Parsons, E. K., Panaousis, E., Loukas, G., & Sakellari, G. (2023). A survey on cyber risk management for the Internet of Things. *Applied Sciences*, 13(15), 9032.

Patel, A.U., Williams, C.L., Hart, S.N., Garcia, C.A., Durant, T.J., Cornish, T.C. and McClintock, D.S., 2023. Cybersecurity and information assurance for the clinical laboratory. *The journal of applied laboratory medicine*, 8(1), pp.145-161.

Plappert, C., Zelle, D., Gadacz, H., Rieke, R., Scheuermann, D., & Krauß, C. (2021, March). Attack surface assessment for cybersecurity engineering in the automotive domain. In: *2021 29th Euromicro international conference on parallel, distributed and network-based processing (PDP)*. IEEE, pp. 266-275.

Potter, L., Ayala, O., & Palmer, X. L. (2021, February). Biocybersecurity: a converging threat as an auxiliary to war. In: *ICCWS 2021 16th international conference on cyber warfare and security*, p. 291.

Potter, L., & Palmer, X. L. (2023). Mission-Aware Differences in Cyberbiosecurity and Biocybersecurity Policies: Prevention, Detection, and Elimination. In: *Cyberbiosecurity*. Springer, Cham, pp. 37-69.

Qiu, J., Li, L., Sun, J., Wei, H., Xu, Z., Lam, K. and Yuan, W., 2025. Emerging cyber attack risks of medical ai agents. *arXiv preprint arXiv:2504.03759*.

Rajora, R., Kumar, A., Malhotra, S. and Sharma, A., 2022, December. Data security breaches and mitigating methods in the healthcare system: A review. In: *2022 International Conference on Computational Modelling, Simulation and Optimization (ICCMSO)*. IEEE, pp. 325-330.

Raković, L., Sakal, M., Matković, P. and Marić, M., 2020. Shadow IT–systematic literature review. *Information Technology and Control*, 49(1), pp.144-160.

Razaque, A., Amsaad, F., Khan, M. J., Hariri, S., Chen, S., Siting, C., & Ji, X. (2019). Survey: Cybersecurity vulnerabilities, attacks and solutions in the medical domain. *IEEE Access*, 7, 168774-168797.

Sadeghi, Z., Alizadehsani, R., Cifci, M.A., Kausar, S., Rehman, R., Mahanta, P., Bora, P.K., Almasri, A., Alkhawaldeh, R.S., Hussain, S. and Alatas, B., 2024. A review of Explainable Artificial Intelligence in healthcare. *Computers and Electrical Engineering*, 118, p.109370.

Silic, M. and Back, A., 2014. Shadow IT–A view from behind the curtain. *Computers & Security*, 45, pp.274-283.

Skorobogatjko, A., Romanovs, A., & Kunicina, N. (2014). State of the Art in the Healthcare Cyber-physical Systems. *Information Technology and Management Science*, 17(1), 126-131.

Spanakis, E. G., Bonomi, S., Sfakianakis, S., Santucci, G., Lenti, S., Sorella, M., ... & Magalini, S. (2020, July). Cyber-attacks and threats for healthcare–a multi-layer thread analysis. In: *2020 42nd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC)*. IEEE, pp. 5705-5708.

Steele, B. J. (2008). *Ontological security in international relations: Self-identity and the IR state*. Routledge.

Sultanovs, E., Skorobogatjko, A., & Romanovs, A. (2016, October). Centralized healthcare cyber-physical system's architecture development. In: *2016 57th International scientific Conference on power and electrical Engineering of Riga Technical University (RTUCON)*. IEEE, pp. 1-6.

Thomson, K. L. (2021). *Cybersecurity: reducing the attack surface*. Nelson Mandela University.

Van Devender, M. and McDonald, J.T., 2023, February. A Quantitative Risk Assessment Framework for the Cybersecurity of Networked Medical Devices. In: *International Conference on Cyber Warfare and Security*, 18(1), pp. 402-411.

Verma, R. (2022). Smart city healthcare cyber physical system: characteristics, technologies and challenges. *Wireless personal communications*, 122(2), 1413-1433.

Wasserman, L. and Wasserman, Y., 2022. Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). *Frontiers in digital health*, 4, p.862221.

Yeo, L.H. and Banfield, J., 2022. Human factors in electronic health records cybersecurity breach: an exploratory analysis. *Perspectives in health information management*, 19(2), p.1i.

Zhang, Y., Qiu, M., Tsai, C. W., Hassan, M. M., & Alamri, A. (2015). Health-CPS: Healthcare cyber-physical system assisted by cloud and big data. *IEEE Systems Journal*, 11(1), 88-95.