The Critical Role of Cybersecurity Education in Health Tourism

Jyri Rajamäki, Paulinus Ofem, Annika Kallio and Miia Vakkuri
Laurea University of Applied Sciences, Espoo, Finland

Jyri.Rajamaki@laurea.fi
Paulinus.Ofem@laurea.fi
Annika.Kallio@laurea.fi
Miia.Vakkuri@laurea.fi

Abstract: Health tourism is expanding due to the availability of high-quality medical care at lower costs in various countries. With this growth comes an increasing need to enhance cybersecurity, as patient data and other sensitive information are vulnerable to cyberattacks, which can lead to identity theft, financial fraud, and privacy breaches. Therefore, robust cybersecurity measures are essential to protect patient data. One challenge is the international transfer of patient data. When patients travel across borders for medical treatment, their data must be securely transmitted between healthcare providers in different countries. This process introduces cybersecurity risks, and healthcare providers must implement strong encryption methods and secure communication channels. This paper discusses the vulnerabilities of information systems used in medical tourism and how they should be considered in higher education teaching. Many healthcare facilities rely on interconnected systems and devices like EHR and IoT to provide efficient care. However, these systems can be susceptible to cyberattacks if not properly secured. A case study on medical tourism in Finland illustrates the practical implications of these cybersecurity challenges. These examples highlight the importance of adopting best practices and successful cybersecurity strategies to safeguard patient information. Recommendations for improving cybersecurity for stakeholders in the medical tourism sector include investing in advanced cybersecurity technologies, providing regular staff training, and developing comprehensive cybersecurity policies. By prioritizing cybersecurity, medical tourism providers can maintain patient safety and trust, which are critical for the continued growth and success of the industry. The importance of cybersecurity training and education in the health and wellness sector and the tourism industry cannot be overstated. Ensuring that all stakeholders are aware of the risks and equipped with the knowledge to mitigate them is essential for protecting patient data and maintaining the integrity of medical tourism services.

Keywords: Health tourism, Cybersecurity, Education, Higher education institute, Case study

1. Introduction

Health tourism is an umbrella term that includes medical and wellbeing tourism. It refers to travel aimed at improving or maintaining health and wellbeing. Health tourism includes various health services, such as medical treatments, rehabilitation, and wellness (Tourism Teacher, 2023). Medical tourism is a subset of health tourism focusing on medical treatments and procedures. Medical tourists often travel abroad for more affordable or more readily available medical services, such as surgeries, dental care, or fertility treatments (Whitlock, 2022). Wellbeing tourism focuses more on holistic well-being and relaxation. Wellbeing tourism can include spa treatments, yoga, meditation, nature retreats, and other relaxing and rejuvenating experiences. The goal is to enhance the traveler's physical and mental well-being (Global Wellness Institute, 2024).

Laurea is a multidisciplinary university of applied sciences (UAS) that educates tourism, healthcare, and cybersecurity students. There is a notable lack of research that integrates these fields. This paper aims to fill this research gap and address the question: "How can cybersecurity in health tourism be effectively integrated and understood within the curricula of multidisciplinary higher education institutions?"

CyberSecrPro is a EU-funded project that aims to encourage higher education institutes (HEIs) to enhance their capacity to prepare a new generation of workforce and to upskill the current workforce to address challenges in the cybersecurity ecosystem. From CyberSecPro's point of view, this paper aims to compile and document best practices for collaboration between HEIs and companies in offering practical training. These best practices will provide guidelines for expanding and delivering cybersecurity training in HEIs.

2. Literature Review

Health tourism, including medical and wellbeing tourism, focuses on improving travellers' physical and mental health. Faced with long waiting lists, the high cost of elective treatment, and fewer barriers to travel, the idea of availing healthcare in another country is gaining more significant appeal to many (Carrera & Bridges, 2006). Health tourism is an important sector of the tourism industry that offers a wide range of services and experiences to travelers, and it provides significant benefits to both travelers and the tourism industry (Zhong et al. 2021). Health tourism can improve travelers' health and well-being, provide new experiences, and help them relax and recover from everyday stress, thus promoting overall well-being. Additionally, this form of

tourism can promote the growth of the tourism industry and create new business opportunities. Health tourism can include various activities such as yoga, meditation, nature retreats, and spa treatments. Health tourism is one of today's thriving industry's most developed and growing sectors. It has increased its activity worldwide due to many social and economic circumstances that lead people to achieve and pursue a better quality of life (Quintela et al., 2016).

Medical tourism involves traveling to another country for medical procedures, such as surgeries, dental treatments, or fertility treatments. This form of tourism is particularly popular in countries where healthcare costs are high or certain treatments are unavailable. Medical tourism allows travelers to receive high-quality care at a more affordable price. However, a significant portion of medical tourism involves short-distance travel across nearby borders and from diasporas, often for less critical medical procedures, which contradicts common perceptions. Despite being part of a growing global medical industry, much of this tourism remains local and diasporic, closely tied to the broader tourism sector. Medical tourism companies, acting as intermediaries, have become increasingly important. Opportunities in this field are primarily spread through word of mouth, with the internet playing a secondary role. The quality and availability of care, along with economic and cultural factors, are major influences on the behavior of medical tourists (Connell, 2012).

Well-being tourism, also known as wellness tourism, integrates aspects of health and medical tourism with a focus on holistic well-being. This includes spa treatments, nutritious food, physical activities, and various wellness programs aimed at enhancing travelers' physical, mental, and emotional health. According to Dini and Pencarel (2021), wellness tourism encompasses ten key components: hot springs, spas, medical tourism, body and mind care, enogastronomy, sports, nature and environment, culture, spirituality, and events. These elements can be offered individually to specific market segments or combined into an integrated mix of tourism products (Dini & Pencarel, 2021).

However, health tourism encounters numerous challenges, one of which is the inconsistency in its various conceptual approaches and definitions (Quintela et al., 2016). On the other hand, a holistic view of wellness tourism impacts strategic marketing processes. Destination management organizations and company managers should segment their demand according to more innovative criteria than those traditionally used for wellness regarding healthcare and medical procedures. Value propositions for tourists should be wellness-driven to meet the growing demand for well-being, and they should involve the participation of all various actors and producers within the wellness tourism offer system at wellness destinations (Dini & Pencarel, 2021).

2.1 New Technologies in Health Tourism

2.1.1 International transfer of patient data

The international transfer of patient data is a crucial aspect of health tourism, but it faces several challenges. One of the primary issues is complying with data protection laws in different countries. For instance, the General Data Protection Regulation (GDPR) in the European Union imposes strict rules on transferring personal data, including health data, outside the EU. This can slow down research and treatment processes as data sharing becomes more complex and requires strict adherence to regulations. Bradford et al. (2020) examine the difficulty of exchanging health data between the USA and the EU and suggest that the United States seek an additional sector-specific adequacy decision based on the existing US health privacy law, the Health Insurance Portability and Accountability Act. This could also serve as a model for other third parties and facilitate the international harmonization of health data exchange.

Cloud computing holds significant promise for revolutionizing the healthcare sector. However, centralizing data in the cloud introduces various security and privacy challenges for patients and healthcare professionals. Maintaining the confidentiality of medical data exchanged between the sender and receiver is essential, which can be achieved through cryptography. It is crucial to employ advanced encryption techniques and secure communication channels to ensure data security. These measures protect patient data from breaches and hacking, which is vital for safeguarding patient privacy. Moreover, secure communication channels ensure that data is transferred swiftly and reliably between healthcare providers, enhancing continuity of care and patient safety (Selvakumar & Lokesh, 2024).

Electronic Health Records (EHR) systems are highly significant in health tourism, offering numerous benefits. They enable healthcare providers to access patient health information in real time, enhancing care coordination and reducing the risk of errors. EHR systems also reduce administrative tasks, such as paperwork, freeing up more time for patient care. By lowering the costs associated with paper-based systems and

preventing duplicate tests, EHR systems can lead to significant savings. Furthermore, patients can access their health information, helping them take a more active role in their care. In health tourism, EHR systems facilitate communication among healthcare providers, enabling better care coordination and reducing medical errors (Adeniyi et al., 2024).

However, there are several challenges associated with the use of EHR systems that can impact their effectiveness and adoption. Protecting patient data is paramount, and EHR systems can be vulnerable to data breaches and hacking. Implementing and maintaining EHR systems can be expensive, particularly for smaller healthcare organizations. Issues such as interoperability, data security, and provider burnout need to be addressed to fully realize the potential of EHRs in improving patient care and outcomes (Adeniyi et al., 2024). The complexity of these systems can pose challenges for healthcare professionals who are not accustomed to using technology. Inaccurate or incomplete data can lead to medical errors and affect patient safety. Additionally, using EHR systems can increase the workload for physicians, leading to burnout, and ongoing efforts are needed to address challenges and ensure the effective use of EHRs in healthcare delivery (Adeniyi et al., 2024).

2.1.2 Internet of medical things (IoMT)

Internet of Medical Things (IoMT) refers to applying the Internet of Things (IoT) in healthcare, enabling medical systems to connect various smart devices, such as wearable sensors, medical examination instruments, and hospital assets, for establishing an information platform (Huang et al., 2023). The Internet of Medical Things (IoMT) technology can be utilized in health tourism in various ways. IoMT devices, such as smart wristbands and other sensors, can monitor patients' health in real-time, allowing for remote diagnostics and treatment planning before the patient arrives at the destination. These devices can store and share patient data securely among different healthcare professionals, ensuring that the patient's medical history is always available, which improves the quality and continuity of care. IoMT devices can send alerts and real-time data in emergencies, enabling quick response and treatment even if the patient is far from home (Mathkor et al., 2024). Remote monitoring and diagnostics can reduce unnecessary doctor visits and hospital stays, making health tourism more cost-effective for patients and healthcare systems. IoMT devices can help patients monitor their health and take a more active role in their care, improving health outcomes and patient satisfaction.

Cybersecurity is a critical factor in using IoMT technology in health tourism. Data security and privacy are essential, as IoMT devices collect and transmit sensitive health information. Cybersecurity measures ensure that these data remain protected and confidential, which is crucial for safeguarding patient privacy. Reliable and uninterrupted operation of IoMT devices is vital, as patients need to trust the information provided by these devices and the care they receive. Cybersecurity helps prevent cyberattacks that could compromise patient safety in emergencies. For example, if IoMT devices are attacked, critical alerts could be prevented from reaching healthcare professionals. Compliance with regulatory requirements is necessary, and cybersecurity ensures that IoMT devices and their use meet these standards, which are essential for adhering to legal and ethical guidelines. When patients know that their health data are protected and that IoMT devices are safe to use, their trust in health tourism services increases, which can improve patient satisfaction and health outcomes. However, risks appearing from IoMT devices cannot easily fit into an existing risk assessment framework. While research has been done on this topic, little attention has been paid to the methodologies used for the risk assessment of heterogeneous IoMT devices (Pritika et al., 2023).

EHR and IoMT systems can be integrated in various ways to enhance healthcare efficiency and patient safety. IoMT devices can collect and transmit patient health data in real-time to EHR systems, enabling continuous monitoring and rapid response to potential health issues. Combining real-time data from IoMT devices with historical patient data in EHR systems allows healthcare professionals to gain a comprehensive view of the patient's health, aiding in more accurate diagnoses and personalized treatment plans. IoMT enables remote monitoring and care, which is particularly beneficial for managing chronic conditions and post-surgery care. Patient data can be updated in EHR systems in real-time, improving continuity of care and reducing the need for physical visits. IoMT devices can send data directly to EHR systems, reducing manual data entry errors and improving data accuracy, which enhances care coordination and patient safety. However, the lack of interoperability hampers the application of new data-processing techniques, such as data mining and online analytical processing, due to the heterogeneity of the data and the sources. Rubí and de Lira Gondi (2019) propose an IoMT platform for pervasive healthcare that ensures interoperability, quality of the detection process, and scalability in a Machine-to-Machin-based architecture and provides functionalities for the processing of high volumes of data, knowledge extraction, and common healthcare services. Their platform

uses the semantics described in OpenEHR for data quality evaluation and standardization of healthcare data stored by the association of IoMT devices and observations defined in OpenEHR (Rubí & de Lira Gondi, 2019).

In summary, integrating EHR and IoMT systems can significantly improve the quality and efficiency of healthcare by providing real-time monitoring, enhanced diagnostics and treatment, and better data security. New technologies in health tourism, such as telemedicine, wearable health technologies, health applications, virtual reality, artificial intelligence, and robotics, can significantly enhance the safety, efficiency, and patient experience. Cross-border EHR systems are key in leveraging these technologies, enabling better data sharing and care coordination across different countries.

2.2 Importance of Cybersecurity in Medical Tourism

Cybersecurity is a crucial part of the tourism industry because it protects the information and systems of travelers and businesses. Information security issues have become an important factor restricting tourism development (Mei et al., 2024). Lázaro's (2024) findings show that hotels and online travel agencies (OTAs) are constantly exposed to cyberattacks, especially by data breaches and malware attacks. These incidents have profound implications for both guests and tourism companies, as their vulnerabilities and consequences impact the reputation of the companies, the smart cities in which they operate, and consumer trust. The findings also revealed that most cyberattacks target the theft of private data belonging to companies and users, including email addresses, credit card numbers, security codes, expiration dates, and encoded magstripe data, among other types of information. Cyberattacks and cyber threats persist in travel and tourism, driven by hackers' desires for power, fame, and wealth (Lázaro, 2024).

Health tourism is an attractive target for cybercriminals since it handles large amounts of personal and financial data. It can be posited that this phenomenon integrates the cybersecurity challenges inherent in both the tourism industry and the medical field. The most common challenges of health tourism include (Briguest, 2024):

- Data breaches and leaks: Protecting patients' personal and medical information is critical, as data breaches can lead to identity theft and other harmful actions.
- Ransomware attacks: Medical institutions can be targeted by ransomware, where attackers encrypt the institution's data and demand a ransom for its release.
- Phishing attacks: Fraudulent messages and websites can trick patients or staff into disclosing sensitive information.

Nowadays, hyperconnectivity allows the tourism industry to leverage big data analytics as a competitive advantage in decision-making, product design, and precise marketing strategies for target segments. However, storing financial, organizational, and personal information in cyberspace and making it accessible to many users also exposes it to security risks such as phishing and hacking, which are common cybercrimes affecting the tourism sector (Arenas-Reséndiz et al., 2024). Due to these challenges, medical tourism services need to invest in strong cybersecurity measures, such as security training, advanced protection systems, and collaboration with authorities.

3. Methodology

This study employs Yin's (2019) case study research method to explore how cybersecurity in health tourism can be effectively integrated into the curricula of multidisciplinary higher education institutions. The research utilizes various data collection methods, including documents, interviews, and observations, to gather comprehensive information and ensure the accuracy of the findings through triangulation. The focus is on understanding cybersecurity training needs within the context of Finland's health tourism industry. The goal is to gain insights and find practical solutions rather than seeking a single truth or broad generalizations. The analysis primarily uses qualitative content analysis to summarize the collected material and identify key themes, relationships, and implications.

Using documents as research material in case studies is a common and effective method for gathering detailed, contextualized information (Yin, 2019). This study's sources of documents include various web pages, CyberSecPro deliverables, and Theseus, Finland's largest open-access repository for theses and publications from universities of applied sciences (AMKIT 2024).

The research seeks new perspectives on cybersecurity education in health tourism, using interviews as a key data collection method. Interviews are versatile and flexible, allowing for direct interaction and uncovering

hidden motives. Open interviews, which are informal and unstructured, aim to explore interviewees' thoughts, opinions, and perceptions.

In this study, professionals from the healthcare and cybersecurity sectors were interviewed:

- Four industry professionals discussed the current state of cybersecurity training and awareness in healthcare, focusing on staff awareness and training sufficiency.
- Three cybersecurity experts shared insights on implementing the European Cybersecurity Skills Framework (ECSF) in healthcare, emphasizing the importance of tailored cybersecurity protocols.

The authors, with extensive experience in healthcare (n=1), tourism (n=1), and cybersecurity (n=2), also contributed their observations to the research.

4. Case Background: Medical Tourism in Finland

Health tourism in Finland dates back to the 18th century, when spas were established, known for their healthy springs and mineral waters. Today, wellness tourism is a significant growth area, with Finland's strengths including clean nature, water, forests, the sauna experience, silence, and light. The COVID-19 pandemic has boosted interest in domestic travel and outdoor activities. (Lehto, 2021)

Medical tourism is also growing, attracting international patients with high-quality healthcare services. Finnish hospitals and clinics offer top-level care, quick access to treatment, and excellent outcomes. Notable examples include Docrates Cancer Center and Orton Oy. The Medical Tourism Association Finland (2025) aims to make Finland the leading medical tourism destination in the Nordic countries, highlighting strengths such as pioneering diagnostics and expert healthcare professionals.

Travel motives in health tourism can be narrow (treatment of illness) or broad (maintaining and promoting health). Wellness tourism motives include relaxation, a change of scenery, and exploring new places. Families with children are a key target group, and they are interested in nature destinations, spas, and active holidays. Their travel motives are influenced by family activities, ease, and safety, with social media playing a significant role in destination choice. Wellness tourism in Finland offers diverse opportunities, especially for families, with important factors being the destination's offerings, price, and ease. Development should consider families' needs and interests. (Lehto, 2021).

5. Findings

5.1 Impact of new Technologies on Health Tourism in Finland

Data Protection Practices and Legislation: International transfer of patient data requires strict adherence to data protection practices and legislation. In Finland, patient data is stored in the Kanta system, ensuring information security and availability. This system also allows for storing and handling patient data from abroad in the same manner as for Finnish patients.

Availability and Compatibility of Patient Data: Transferring patient data from abroad to Finland can improve the quality and continuity of care, as healthcare professionals can access necessary information about the patient's previous treatments. However, this requires that patient information systems are compatible and that data can be translated into the required languages.

Cybersecurity and Trust: International transfer of patient data demands high cybersecurity to maintain patient privacy and trust. This is particularly important in health tourism, where patients may be concerned about the security and use of their data.

Practical Challenges and Opportunities: Practical challenges of international patient data transfer include differences in legislation and data protection practices between countries. On the other hand, efficient data transfer can enhance the attractiveness and competitiveness of health tourism, as patients can trust they will receive high-quality care abroad.

Internet of Medical Things (IoMT):

- Enhanced Patient Monitoring and Management: Given Finland's advanced healthcare infrastructure, IoMT can significantly improve patient monitoring and management for international patients. This ensures personalized and high-quality care, a key attraction for health tourists.

- Security and Privacy Concerns: Finland strongly emphasizes data protection and privacy. Ensuring the cybersecurity of IoMT devices and systems is crucial to maintaining patient trust and complying with stringent data protection regulations.
- Interoperability and Integration: The ability to seamlessly integrate IoMT devices with existing healthcare systems is vital. Finland's robust digital health infrastructure can support the interoperability needed to provide continuous and coordinated care for international patients.
- Regulatory and Compliance Issues: Navigating the regulatory landscape is essential. Finland's adherence to high medical device regulation and data protection standards ensures that IoMT implementations meet international requirements, making it a reliable destination for health tourists.

The above-mentioned aspects highlight how IoMT can enhance the quality and security of health tourism services in Finland, making it an attractive destination for international patients. Our findings also indicate that international transfer of patient data can significantly impact health tourism in Finland by improving the quality of care and patient trust while also posing challenges related to cybersecurity and compliance with legislation.

5.2 CyberSecrPro as Best Practice for Cybersecurity Workforce Skills Training

In order to fulfil its aim, the CyberSecPro project performed a market analysis of cybersecurity workforce skills in the EU. The market analysis report (Rathod et al., 2023) identified over 25 essential cybersecurity knowledge areas for health, energy, maritime and other sectors. It also identified over 25 workforce skills in demand in these major sectors. One of the significant outcomes of the study is the workforce skills gap between HEIs cybersecurity programs and workforce skills needed in the labour market. Through desk research, it was confirmed that the demand for skilled cybersecurity professionals surpasses the supply of cybersecurity professionals.

In addition to performing a cybersecurity market-driven analysis, it was instructive to analyse the cybersecurity education programs of all consortium partners and the tools they utilise to enhance their respective academic programs. The full report of the analyses is provided in (Lugo et al., 2023). Consortium partners' courses were evaluated for their applicability to different cybersecurity knowledge skills areas identified by Rathod et al., 2023. The courses were also matched with the European Cybersecurity Skills Framework (ECSF) to determine their level of coverage and alignment with the ECSF. However, it was found that while some courses covered the ECSF, several poorly covered the ECSF.

Based on the findings in (Rathod et al., 2023) and (Lugo et al., 2023), it was highly recommended that HEIs transform their academic offerings to address the cybersecurity workforce market challenges and increase investment in cybersecurity education and professional training. HEI providers should also collaborate with industry practitioners to enhance the cybersecurity workforce skills of all stakeholders in the ecosystem. HEIs' course materials and resources should also be revamped, considering continuous industry development and emerging technologies.

Informed by previous outcomes, relevance to ECSF, the availability of education and training resources, and the need to protect EU cyber-infrastructure and systems effectively, CyberSecPro further developed its professional cybersecurity training program requirements and various specifications (Lieberknecht et al., 2023). It identified 10 cybersecurity knowledge areas relevant to CyberSecPro's workforce skills development. To ensure that the CyberSecPro program is created based on well-established resources and expertise, current partners' academic offerings were mapped to the identified knowledge areas and essential selected cybersecurity training modules. The report also provides an analysis of the constraints and requirements necessary for the adoption of the CyberSecPro professional training program. These analyses include business, technical, legal, social and financial aspects. These outcomes served as the basis for further developing CyberSecPro's cybersecurity training modules. A dynamic curriculum management system (DCM) was proposed to enhance the training and make training resources available to trainees and trainers.

Armed with the lessons, recommendations and other outcomes from (Rathod et al., 2023; Lugo et al., 2023; Lieberknecht et al., 2023), especially the CyberSecrPro requirements and specifications, D3.1 embarked on the actual development of CyberSecPro's main components and procedures. In this vein, 12 generic cybersecurity training modules were developed to enable trainees to gain the essential knowledge and skills required to succeed. These modules broadly cover the essentials and management of cybersecurity, emerging technologies and critical infrastructure security. The generic modules offer a firm foundation for cybersecurity principles and practices, a core cybersecurity capability within the CyberSecPro portfolio. The key concepts

included in these modules are threat intelligence, software and network security, data protection and privacy technologies, penetration testing, and risk management.

To address sector-specific training needs, CyberSecPro further developed a cybersecurity model syllabus for health (Kerllegis et al., 2024), energy (Alcaraz et al., 2024), and maritime (Kerllegis et al., 2024). The training modules for these targeted sectors are geared towards the peculiar cybersecurity challenges in these sectors, and trainees are equipped with knowledge, skills, and competencies to combat cybersecurity threats and vulnerabilities. A streamlined enrolment procedure was established to enable the recruitment and participation of targeted individuals in the program. The DCM facilitates this procedure. As part of efforts to enhance trainers' efficiency and organization, several templates and e-forms were developed in support of administrative processes. These templates include registration forms, trainers' and trainees' evaluation forms, and teaching materials, among others.

CyberSecPro developed and deployed the Dynamic Curriculum Management (DCM) system to ensure the training program remains relevant and up-to-date with the evolving cybersecurity ecosystem. The DCM helps keep the training content current and allows for identifying and monitoring cybersecurity labor market trends, emerging threats, and vulnerabilities.

Concerning the healthcare sector's cybersecurity training needs, as established in (Rathod et al., 2023), CyberSecPro developed a portfolio of curricula and syllabi to enhance the cybersecurity workforce skills of healthcare professionals. The specialized cybersecurity modules developed are based on the 12 CyberSecPro core modules and the specific training requirements in health. The training modules cover a range of cybersecurity themes, such as human factors of cybersecurity, data and privacy security and a host of other topics. With this training, healthcare professionals are empowered to deploy the necessary tools, technologies, and expertise to secure and protect patient data and preserve the system's integrity. Table 1 summarizes the training modules developed for health sector cybersecurity.

Table 1: Summary of CyberSecPro training modules for the health sector

S/N	Module Code	Module Title
1	CSP001_W_H	Cybersecurity Essentials and Management for Health Sector
2	CSP001_CS-E_H	RxB - Cyber security management game
3	CSP002_S_H	Cybersecurity and Health
4	CSP002_SA_H	Human Aspects of Healthcare Cybersecurity
5	CSP003_C_H	Cybersecurity Risk Management and Governance in the Healthcare sector
6	CSP004_C_H	Network Security for Health
7	CSP004_S_H	Cybersecurity - Endpoint protection in healthcare systems
8	CSP005_S_H	Data Protection and Privacy Technologies for Healthcare
9	CSP005_W_H	Data Protection and Privacy Technologies for Healthcare
10	CSP006_SA_H	Cyber Threat Intelligence for Healthcare
11	CSP006_S_H	Network and IoMT Security
12	CSP007_S_H	Practical Insights in Anomaly Detection
13	CSP007_SA_H	Cybersecurity in Emerging Technologies, in particular explainable AI for healthcare
14	CSP008_S_H	Cascading Effects in Complex Health Networks
15	CSP009_W_H	Securing Healthcare Web Applications
16	CSP0010_W_H	Penetration Testing for Healthcare IT Infrastructures
18	CSP0011_S_H	Cyber Ranges and Operations in healthcare domain
19	CSP0011_W_H	Detection Engineering on a Cyber Range of a Healthcare IT infrastructure-Active Directory
20	CSP0012_SA_H	Digital Forensics for Health Sector
21	CSP012_S_H	Digital Forensics for Health

In CyberSecPro, a training module could be a course (C), seminar (S), workshop (W), cybersecurity exercise (CE), summer school (SS), winter school (WS), and hackathon (H). These module types are indicated in the module code (see Table 1, column 2) generation, and the last letter (H) in the code represents health (i.e., health training module). Training modules in other sectors are similarly named. To ensure the quality of the training modules, trainers and trainees evaluate each implemented module, and the feedback generated from the evaluation is utilized to improve future implementations.

Creating an operational training plan (Koloudu et al., 2024) that encompasses mobilizing potential trainees and trainers to implement these CyberSecPro training modules successfully is important. The operational plan enabled the operationalization of the generic and sector-specific cybersecurity training modules, which provide basic and advanced competence levels. Currently, the implementation of the training modules is ongoing even as new modules are introduced.

6. Conclusions

The integration of cybersecurity in health tourism is crucial for ensuring the safety and privacy of patient data, which is increasingly vulnerable to cyberattacks. This paper has highlighted the importance of addressing cybersecurity within multidisciplinary higher education institutions (HEIs) curricula to prepare a skilled workforce capable of managing these challenges. Our findings indicate that the international transfer of patient data and the use of interconnected systems, such as Electronic Health Records (EHR) and the Internet of Medical Things (IoMT), bring significant benefits to health tourism but also present significant cybersecurity risks. These risks must be mitigated through robust security measures, including advanced encryption techniques, secure communication channels, and comprehensive cybersecurity policies.

The CyberSecPro project serves as a best practice model for developing and implementing cybersecurity training programs tailored to the needs of the healthcare sector, which can also be utilized in health tourism education. By aligning educational offerings with the European Cybersecurity Skills Framework (ECSF) and continuously updating training content to reflect emerging threats and technologies, HEIs can better equip their students with the necessary skills and knowledge. The effective integration of cybersecurity in health tourism education requires a collaborative approach between academia and industry. HEIs must transform their academic offerings to address the evolving cybersecurity landscape and invest in continuous professional development. By doing so, they can ensure that future healthcare professionals are well-prepared to protect patient data and maintain the integrity of health tourism services.

Acknowledgement

The authors would like to acknowledge the financial support provided by the following projects: CyberSecPro: Collaborative, Multi-modal, and Agile Professional Cybersecurity Training Program for a Skilled Workforce in the European Digital Single Market and Industries, which have received funding from the European Union's Digital Europe Programme (DEP) under grant agreements No. 101083594. The views expressed in this paper represent only the authors' views and not those of the European Commission or the partners in the CyberSecPro project. Finally, the authors declare that no conflicts of interest, including any financial or personal relationships, could be perceived as potential conflicts.

References

Adeniyi, Adekunle Oyeyemi, et al. “The Impact of Electronic Health Records on Patient Care and Outcomes: A Comprehensive Review.” World Journal of Advanced Research and Reviews, vol. 21, no. 2, Feb. 2024, pp. 1446–55, doi:10.30574/wjarr.2024.21.2.0592.

Alcaraz, C. et al. (2024) “CyberSecPro Portfolio of Cybersecurity Curricula Targeted to Energy,” 2023. [Online]. Available: https://www.cybersecpro-project.eu/wp-content/uploads/2024/06/D3.4-V1.1-Re-submitted-.pdf

AMKIT. 2024. Theseus. Online: https://www.amkit.fi/en/theseus-en/ Referred 25 Jan., 2025.

Arenas-Reséndiz, Tanya, et al. “Methodology to Analyse Cybersecurity in Tourism.” Smart Tourism, vol. 5, no. 1, Mar. 2024, pp. 2495–2495, doi:10.54517/st.v5i1.2495.

Bradford, Laura, et al. “International Transfers of Health Data between the EU and USA: A Sector-Specific Approach for the USA to Ensure an ‘Adequate’ Level of Protection.” Journal of Law and the Biosciences, vol. 7, no. 1, Jan. 2020, doi:10.1093/jlb/lsaa055.

Briguest, “Cybersecurity Challenges in Tourism: Emerging Threats and Vulnerabilities,” 13 August 2024. Available: https://www.briguest.com/en/cybersecurity-challenges-tourism-emerging-threats-vulnerabilities/ Referred 25 Jan., 2025.

Carrera, Percivil Melendez, and John F. P. Bridges. “Globalization and Healthcare: Understanding Health and Medical Tourism.” Expert Review of Pharmacoeconomics & Outcomes Research, vol. 6, no. 4, Aug. 2006, pp. 447–54, doi:10.1586/14737167.6.4.447.

Connell, John. “Contemporary Medical Tourism: Conceptualisation, Culture and Commodification.” Tourism Management, vol. 34, June 2012, pp. 1–13, doi:10.1016/j.tourman.2012.05.009.

Dini, Mauro, and Tonino Pencarelli. “Wellness Tourism and the Components of Its Offer System: A Holistic Perspective.” Tourism Review, vol. 77, no. 2, July 2021, pp. 394–412, doi:10.1108/tr-08-2020-0373.

Florido-Benítez, Lázaro. “The Cybersecurity Applied by Online Travel Agencies and Hotels to Protect Users’ Private Data in Smart Cities.” Smart Cities, vol. 7, no. 1, Feb. 2024, pp. 475–95, doi:10.3390/smartcities7010019.

Global Wellness Institute, Wellness Policy Toolkit: Wellness In Tourism, 2024 https://globalwellnessinstitute.org/industry-research/2024-wellness-policy-toolkit-wellness-in-tourism/

Hirsjärvi, S., Remes, P. and Sajavaara, P. Tutki ja kirjoita, Keuruu: Otava, 2007.

Huang, Chenxi, et al. “Internet of Medical Things: A Systematic Review.” Neurocomputing, vol. 557, Aug. 2023, pp. 126719–126719, doi:10.1016/j.neucom.2023.126719.

Kaloudi, N. et al. (2024) “CyberSecPro Training Operational Plan,” 2024. [Online]. Available: https://www.cybersecpro-project.eu/wp-content/uploads/2024/05/D4.1-Training-Operational-Plan-v0.1.pdf

Kerllegis, D. et al. (2024) “CyberSecPro Portfolio of Cybersecurity Curricula Targeted to Maritime,” 2023. [Online]. Available: https://www.cybersecpro-project.eu/wp-content/uploads/2024/06/D3.5.-Submitted-2024-06-04.pdf

Koutras, D. et al. (2024) “CyberSecPro Portfolio of Cybersecurity Curricula Targeted to Health,” 2023. [Online]. Available: https://www.cybersecpro-project.eu/wp-content/uploads/2024/06/D3.3-CyberSecPro_Health_v1.0_FINAL_submitted.pdf

Lieberknecht, A. et al. (2024) “CyberSecPro Programme Specifications,” 2023. [Online]. Available: https://www.cybersecpro-project.eu/wp-content/uploads/2024/05/D2.3-CyberSecPro-Programme-Specifications-1.0.pdf

Lehto, T. (2021). Terveysmatkailu Suomessa. Thesis. Haaga-Helia University of applied Sciences.

Lugo, R. et al. (2023) “Blended CyberSecPro technological training interactive technologies and academic practice,” 2023. [Online]. Available: https://www.cybersecpro-project.eu/wp-content/uploads/2024/05/D2.2-Blended-CyberSecPro-technological-training-interactive-technologies-and-academic-practice-v1.0_Submitted.pdf.

Mathkor, Darin Mansor, et al. “Multirole of the Internet of Medical Things (IoMT) in Biomedical Systems for Managing Smart Healthcare Systems: An Overview of Current and Future Innovative Trends.” Journal of Infection and Public Health, Jan. 2024, doi:10.1016/j.jiph.2024.01.013.

Medical Tourism Association Finland, 2025 https://medicaltourismfinland.com/

Mei, Anqi, et al. “Research on Information Security Protection in The Context of Post-Epidemic Tourism Revival.” International Journal of Education and Humanities, vol. 12, no. 2, Feb. 2024, pp. 44–48, doi:10.54097/zwbmyt93.

Pritika, Pritika, et al. “Risk Assessment of Heterogeneous IoMT Devices: A Review.” Technologies, vol. 11, no. 1, Feb. 2023, pp. 31–31, doi:10.3390/technologies11010031.

Quintela, Joana A., et al. “Health, Wellness and Medical Tourism - a Conceptual Approach.” ENLIGHTENING TOURISM A PATHMAKING JOURNAL, vol. 6, no. 1, June 2016, pp. 1–18, doi:10.33776/et.v6i1.2814.

Rathod, P. et al. (2023) “Cybersecurity practical skills gaps in Europe: Market demand and analysis,” 2023. [Online]. Available: https://www.cybersecpro-project.eu/wp-content/uploads/2023/07/D2.1_Cybersecurity_Practical_Skills_Gaps_in_Europe_v.1.0.pdf.

Rubí, Jesús N. S., and Paulo Roberto de Lira Gondim. “IoMT Platform for Pervasive Healthcare Data Aggregation, Processing, and Sharing Based on OneM2M and OpenEHR.” Sensors, vol. 19, no. 19, Oct. 2019, pp. 4283–4283, doi:10.3390/s19194283.

Selvakumar, Kumaravel, and S. Lokesh. “A Cryptographic Method to Have a Secure Communication of Health Care Digital Data into the Cloud.” Automatika, vol. 65, no. 1, Jan. 2024, pp. 373–86, doi:10.1080/00051144.2023.2301240.

Tourism Teacher, What is health tourism and why is it growing? https://tourismteacher.com/health-tourism/ Last updated: 20/01/2023

Whitlock, Jennifer. “Why Patients Are Turning to Medical Tourism” Verywell Health, August 11, 2022 https://www.verywellhealth.com/understanding-medical-tourism-4069869

Zhong, Lina, et al. “Medical, Health and Wellness Tourism Research—A Review of the Literature (1970–2020) and Research Agenda.” International Journal of Environmental Research and Public Health, vol. 18, no. 20, Oct. 2021, pp. 10875–10875, doi:10.3390/ijerph182010875.

Yin, Robert. Case study research: Design and methods (Ed. 4), Thousand Oaks: Sage, 2009.