Designing Modular Cybersecurity Education for Healthcare: Integrating XiA and ManagiDiTH Frameworks with CyberSecPro Insights

Jyri Rajamäki[1] and Jussi Simola[2]
[1]Laurea University of Applied Sciences, Espoo, Finland
[2]University of Jyväskylä, Finland

jyri.rajamaki@laurea.fi
simolajussi@gmail.com

Abstract: The healthcare sector faces increasingly complex cybersecurity threats due to its rapid digital transformation, including the adoption of electronic health records (EHRs), connected medical devices, and telehealth services. This paper presents a modular and interdisciplinary model for cybersecurity education tailored to healthcare professionals. The model integrates three EU-funded initiatives: the XiA Framework's microlearning approach, the ManagiDiTH master's programme's strategic and human-centric curriculum, and the CyberSecPro project's hands-on, scenario-based training modules. Together, these components form a comprehensive educational ecosystem that supports continuous professional development, microcredentialing, and alignment with European standards such as the European Qualifications Framework (EQF), the NIST Cybersecurity Framework, and ENISA's European Cybersecurity Skills Framework (ECSF). The paper outlines the pedagogical foundations of microlearning, the structure of Micro-Content Learning Blocks (MCLBs), and the curriculum design principles that foster cyber resilience in healthcare. It concludes with a discussion on implementation potential, impact indicators, and future directions for research and practice.

Keywords: Cybersecurity education, Healthcare cybersecurity, Microlearning, Microcredentials, European cybersecurity skills framework (ECSF)

1. Introduction

The digital transformation of healthcare has brought significant advancements in patient care, diagnostics, and operational efficiency. However, this evolution has also introduced complex cybersecurity challenges that threaten the integrity, confidentiality, and availability of health data. Hospitals and healthcare organizations are increasingly targeted by cyberattacks, including phishing, ransomware, and Distributed Denial of Service (DDoS) attacks, which can disrupt critical services and compromise sensitive patient information (Priestman *et al.*, 2019; Zhou *et al.*, 2024).

Despite growing awareness, traditional security measures remain insufficient to address the evolving threat landscape. Artificial intelligence (AI) offers promising capabilities for enhancing cybersecurity in healthcare by enabling proactive threat detection and adaptive response mechanisms. AI-driven tools, such as SecureAI, demonstrate how learning from historical patterns can help identify anomalous network behaviors and mitigate risks in real-time (Rajamäki, Nepal and Chalkias, 2025). Healthcare organizations, particularly private entities, often lag behind other sectors in implementing robust cybersecurity frameworks (Tavares, Sousa and Proença, 2024). The urgency to adopt AI-based solutions is underscored by the increasing complexity of digital health infrastructures and the growing reliance on interconnected systems, such as the Internet of Medical Things (IoMT). Aljanabi (2023) illustrates how trustworthy AI techniques can harden intrusion detection systems against data poisoning threats, ensuring continuity of care even under hostile conditions. However, the integration of AI into healthcare cybersecurity is not without ethical and regulatory concerns. Issues such as algorithmic bias, lack of transparency, and accountability must be addressed through comprehensive governance frameworks. Zhang and Zhang (2023) advocate for ethical and legal mechanisms that align with the EU AI Act, which classifies medical AI applications as high-risk and mandates stringent standards for safety and reliability. Moreover, safeguarding patient data requires advanced privacy-preserving techniques. Approaches such as anonymization, differential privacy, and secure multiparty computation are essential for balancing data utility with confidentiality (Ezeah, 2024; Forood *et al.*, 2024). These methods are particularly critical in domains like cancer care, where AI-based diagnostics and precision medicine rely heavily on sensitive health information.

To address the abovementioned challenges, healthcare professionals must be equipped with specialised cybersecurity competencies. This paper proposes a modular education model that integrates the XiA Framework's microlearning approach (XiA, 2025), the interdisciplinary structure of the ManagiDiTH master's programme (ManagiDiTH, 2025), and the market-driven insights of the CyberSecPro project (CyberSecPro, 2025). The remainder of the paper is structured as follows: Section 2 outlines the research methodology,

including the design-based approach and comparative analysis used to synthesize the three educational frameworks. Section 3 presents an in-depth overview of the XiA, ManagiDiTH, and CyberSecPro initiatives, highlighting their pedagogical strategies, thematic coverage, and alignment with European standards. Section 4 focuses on the development of Micro-Content Learning Blocks (MCLBs) for cybersecurity education, providing a detailed examination of their structure and learning outcomes, and elucidating the pedagogical foundations of microlearning in healthcare cybersecurity with particular emphasis on learner-centered design, EQF compatibility, and the support of continuous professional development. Section 5 offers a discussion, reflecting on the model's implementation potential and future directions for research and practice. Finally, Section 6 concludes the paper.

2. Research Methodology

This study employs a qualitative, design-based research methodology as the foundation for developing a modular cybersecurity education model for the healthcare sector. The approach combines document analysis, framework synthesis, and comparative evaluation across three EU-funded projects: XiA, ManagiDiTH, and CyberSecPro. These are selected because the EU-level need of the standardized interoperability in accordance with cybersecurity requirements. The primary method is document analysis, which involves systematic examination of project deliverables, curriculum frameworks, and academic publications. This method is well-established in educational research for extracting structured insights from policy and pedagogical documents (Bowen, 2009). The analysis focused on the pedagogical foundations of micro-content learning and on curriculum design in healthcare cybersecurity. Of the analyzed projects, two (CyberSecPro and ManagiDiTH) have already published their results in openly accessible deliverables and scientific publications, whereas one project launched this year (XiA), does not yet have such materials available. Therefore, the first two projects were analyzed based on public documents, while the analysis of the third relied on internal project working papers.

A comparative case study approach (Yin, 2018) was used to evaluate the similarities and differences between the three initiatives. This included mapping cybersecurity content across modules, identifying target learner profiles, and assessing pedagogical coherence. The comparison informed the integration strategy proposed in the paper, ensuring that the resulting curriculum model reflects best practices and addresses sector-specific needs. Furthermore, the study applies a design-based research (DBR) methodology (Wang and Hannafin, 2005; Reeves, 2006), which is particularly suitable for developing educational interventions in real-world contexts. DBR allows for iterative refinement of the curriculum model through synthesis of theory and practice, guided by principles of microlearning, human-centric cybersecurity, and continuous professional development.

The proposed model is validated through conceptual alignment with recognized educational standards such as the European Qualifications Framework – EQF (European Parliament, 2017), the Finnish National Framework for Qualifications and Other Competence Modules – FiNQF (EDUFI, 2025), the European Cybersecurity Skills Framework – ECSF (ENISA, 2022), and the NIST Cybersecurity Framework (NIST, 2013). While empirical testing is beyond the scope of this paper, future research may include pilot implementations, learner feedback, and impact assessment using key performance indicators such as skill acquisition, incident response capability, and professional mobility.

3. EU-Level Educational Initiatives in Healthcare Cybersecurity

As the healthcare sector undergoes rapid digital transformation, the need for robust cybersecurity competencies has become increasingly urgent. In response, the European Union has launched several strategic educational initiatives aimed at strengthening cybersecurity skills across healthcare professionals, students, and institutions. This section highlights three key projects that contribute to building a resilient and well-trained workforce in digital health. The CyberSecPro Project aims to advance cybersecurity education, with healthcare being one of its three primary domains. In contrast, ManagiDiTH and XiA are development projects focused on digital health education, within which cybersecurity plays a significant role. There is no similar example where cybersecurity challenges of healthcare sector has taken into account by utilizing EU-level requirements and project frameworks in this way. Laurea university of applied sciences engages in development work in all mentioned projects.

Figure 1 illustrates the ecosystem of healthcare cybersecurity education, highlighting the relationships between the CyberSecPro, ManagiDiTH, and XiA projects.

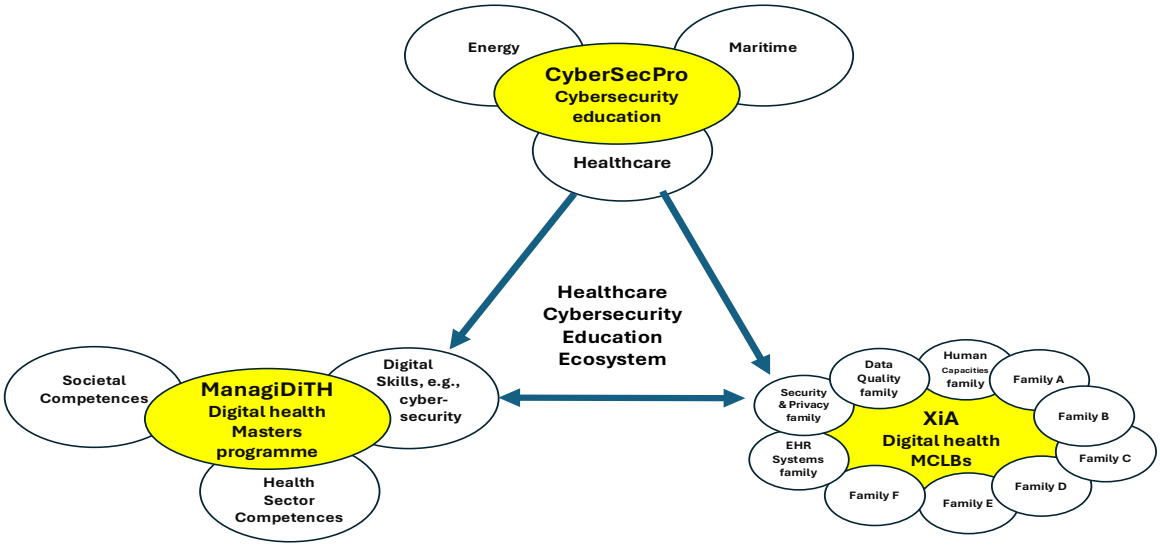

Figure 1: Ecosystem of healthcare cybersecurity education: Relationships between CyberSecPro, ManagiDiTH, and XiA Projects

3.1 CyberSecPro

The CyberSecPro Project is an EU-funded initiative under the Digital Europe Programme, aimed at developing advanced cybersecurity competencies across critical sectors. It covers a wide range of topics, including cybersecurity principles, risk management, security tools, ethical hacking, and incident response. A key focus of the project is human-centric cybersecurity, which recognizes the importance of user behavior, awareness, and ethical considerations in maintaining secure systems. The initiative also promotes continuous professional development, ensuring that professionals remain equipped to handle emerging threats and technologies.

The project's comprehensive market analysis revealed significant gaps in cybersecurity readiness within healthcare, prompting the development of targeted training modules (Rathod *et al.*, 2023). Therefore, a comprehensive portfolio of cybersecurity training modules was tailored to the healthcare sector (Koutras, *et al.*, 2024). This initiative responds to the growing need for healthcare professionals to acquire practical cybersecurity skills to protect sensitive patient data and ensure the integrity of digital health systems. The curriculum is structured into twelve thematic modules, each addressing critical aspects of cybersecurity in healthcare. These modules cover a wide range of topics, including cybersecurity management, human factors, risk governance, network security, data protection, threat intelligence, emerging technologies, infrastructure security, software security, penetration testing, cyber range operations, and digital forensics. Each module is designed to combine both generic cybersecurity principles and healthcare-specific challenges. For example, the module on *Cybersecurity Essentials and Management for Health Sector* introduces foundational concepts such as threat landscapes, regulatory frameworks, and risk mitigation strategies, while also incorporating healthcare-specific case studies and simulations. Similarly, the module on *Human Factors and Cybersecurity for Health* explores psychological and behavioral dimensions of cybersecurity, emphasizing the role of healthcare staff in maintaining cyber hygiene and preventing insider threats (Koutras, *et al.*, 2024).

The training materials emphasize hands-on learning through interactive exercises, simulations, and gamified environments. Modules such as *Cybersecurity Risk Management and Governance* and *Penetration Testing for Healthcare IT Infrastructures* provide learners with practical tools to assess vulnerabilities, implement security controls, and respond to incidents. The inclusion of cyber range environments allows participants to engage in realistic scenarios, simulating attacks and defenses within healthcare IT infrastructures. CyberSecPro also addresses emerging challenges by integrating modules on *Cybersecurity in Emerging Technologies*, including explainable AI and anomaly detection, and *Critical Infrastructure Security*, which examines cascading effects in complex health networks. These modules prepare healthcare professionals to anticipate and respond to future threats in increasingly interconnected and data-driven environments. The curriculum is aligned with European cybersecurity frameworks, including the European Cybersecurity Skills Framework (ECSF), ensuring that the training supports recognized competencies and career pathways. The modular design allows for flexible implementation across academic institutions, professional training programs, and continuing education initiatives (Koutras, *et al.*, 2024).

By offering a holistic and sector-specific approach to cybersecurity education, CyberSecPro empowers healthcare providers to make informed decisions, adopt best practices, and foster a culture of security within their organizations. The project contributes to strengthening the cybersecurity posture of the healthcare sector across Europe, supporting both individual skill development and systemic resilience (Koutras, *et al.*, 2024).

3.2 ManagiDiTH

The ManagiDiTH Programme is a joint master's degree initiative involving universities from three EU member states. It offers a multidisciplinary curriculum that integrates health sector expertise, societal competencies, and digital skills. Within the digital skills track, students may specialize in data science or interoperability, making the programme highly relevant to the evolving requirements of healthcare systems. ManagiDiTH emphasizes cross-border collaboration and mobility, preparing graduates to operate in diverse healthcare environments across Europe (ManagiDiTH, 2025).

The cybersecurity studies within the programme encompass both technical and strategic domains, equipping students with the capabilities to conduct risk assessments, implement protective measures, and participate in the development of digital health governance policies. Cybersecurity is addressed through a dedicated study unit titled *Cybersecurity for Health Systems* (6 ECTS), which provides students with a comprehensive understanding of the unique cybersecurity challenges in healthcare. The course covers the fundamentals of cybersecurity, including risk assessment and management. Students are trained to identify threats, implement safeguards, detect anomalies, respond to incidents, and recover systems. Topics include network and application security, secure cloud computing, medical device protection, governance and compliance, as well as future trends in healthcare cybersecurity. Students also learn to stay informed about emerging cybersecurity trends and technologies, while considering ethical implications and best practices in the healthcare sector. The cybersecurity curriculum is aligned with international standards, such as ECSF and NIST (Rajamäki *et al.*, 2024).

In addition to this core module, cybersecurity themes are embedded across several other study units. For example, *the Managing the Digital Transformation in Healthcare* unit explores ethical and privacy considerations in the use of digital tools. *The Health Data and Information Systems* unit addresses data standards, analytics, and legal frameworks related to health information. *The Regulation, Legislation and Structures in Health* unit examines EU-level digital health governance and its implications for public and private service providers. *The Ethics and Privacy in Health* unit focuses on GDPR compliance and privacy protection. Other units, such as *E-Health and Telemedicine, Interoperable Ecosystems in Health,* and *Emerging Technologies in Interoperability*, also include content related to security and privacy (Rajamäki *et al.*, 2024).

ManagiDiTH adopts a human-centric approach to cybersecurity, recognizing that human behavior is often the weakest link. Based on Grobler's, Gaire's and Nepal's (2021) 3U model (User, Usage, Usability), the curriculum emphasizes situational awareness, psychological and cognitive factors, legal and technical measures, and user experience design. This ensures that students understand not only the technical aspects of cybersecurity but also the human and organizational dimensions. Especially in Internet of Medical Things (IoMT) environments, where numerous interconnected medical devices and systems increase both technical and human vulnerabilities, a comprehensive understanding of user behavior, device usage, and usability becomes particularly important (Rajamäki and Postolache, 2025).

ManagiDiTH emphasizes hands-on learning through case studies and practical exercises, fostering the real-world application of cybersecurity principles. The programme encourages collaboration between educational institutions, healthcare organizations, and cybersecurity experts to ensure relevance and adaptability. Continuous professional development is supported through ongoing training and curriculum updates, and ethical values are reinforced to promote responsible cybersecurity practices. This comprehensive and interdisciplinary approach positions ManagiDiTH as a model for cybersecurity education in healthcare, addressing both current challenges and future needs in a rapidly evolving digital landscape.

3.3 XiA Framework

The XiA framework is a European educational model developed to support the digital transformation of healthcare through modular and flexible learning. It utilizes Micro-Content Learning Blocks (MCLBs), which are short, targeted learning units. These blocks are designed to support micro-credentials, enabling learners to build their competencies in a stackable and customizable manner. The framework is particularly suitable for professionals who require continuous education in rapidly evolving fields such as cybersecurity. Through personalized learning pathways, XiA enables the acquisition of specialized digital health skills without the need

for full degree programs. This approach is ideal for healthcare workers who wish to advance their expertise while remaining active in clinical or administrative roles.

All XiA MCLBs are mapped to EQF levels 5–7, ensuring consistency and recognition across different educational systems. This alignment supports the development of technical and analytical skills (EQF 5–6) for cybersecurity implementation, as well as strategic and leadership competencies (EQF 7) for managing digital transformation in healthcare.

The XiA framework includes a dedicated MCLB family called *Security & Privacy*, which focuses on cybersecurity and data protection in the context of digital health interoperability. This thematic family addresses several critical areas, such as compliance with data protection regulations (e.g., GDPR and HIPAA). It also covers techniques for data anonymization and pseudonymization, implementation of audit trails and access logs, and methods for privacy-preserving cross-border data exchange. Additionally, the content emphasizes building trust between clinicians and patients by ensuring secure and transparent data handling. Within the XiA framework, cybersecurity is regarded as a fundamental requirement for developing reliable and sustainable digital health infrastructures.

The pedagogical design of the XiA framework is based on learner-centeredness, modularity, and competency-based education principles. These principles are essential for addressing the dynamic learning needs of healthcare professionals, especially in the context of cybersecurity, where technological advancements require continuous skill updates. Each XiA MCLB is designed with a clear pedagogical structure that supports effective learning. Modules promote active engagement through simulations, discussions, and problem-solving tasks. Learning progress and competencies are continuously monitored using both formative and summative assessments. Furthermore, multimedia content is integrated to enrich the learning experience and accommodate diverse learning styles.

Cybersecurity is systematically embedded in the competency profiles defined for three key target groups: IT professionals (designers), healthcare and IT management (managers), and healthcare practitioners (end-users). Particular emphasis is placed on competencies related to the responsible handling of health data. These competencies include secure data storage and anonymization techniques, cybersecurity practices such as encryption and access management, knowledge of relevant legislation (GDPR, HIPAA), and mastery of ethical frameworks for the use of artificial intelligence in clinical environments. By integrating these elements, the XiA framework ensures that cybersecurity is addressed not only as a technical skill but also as a core professional responsibility across various roles in healthcare.

Competency-based learning ensures that each block supports practical skills, such as secure data handling, ethical decision-making, and interdisciplinary collaboration. Learning outcomes are recognized through micro-credentials, which validate competencies and enhance employability. These micro-credentials are awarded based on workload and learning outcomes and may be issued by universities or other accredited bodies. They serve as tangible evidence of skills and can be combined into broader qualifications.

In addition to the Security & Privacy family, cybersecurity is addressed in several other MCLB families. For example, the *Data Quality* family focuses on data integrity and its critical role in ensuring the safety and reliability of AI applications in healthcare. The *Electronic Health Record (EHR) Systems* family examines the secure architecture and regulatory aspects of electronic patient record systems. The *Human Capacities* family highlights organizational change management and capacity building to support secure digital transformation. This cross-cutting integration ensures that cybersecurity is not treated solely as a technical issue but is embedded within broader organizational and systemic contexts, reinforcing its significance across multiple domains of digital health education.

To ensure pedagogical integrity, XiA provides a standardized template for MCLB development. The template includes clearly defined learning objectives and corresponding EQF levels, identification of target groups, specification of assessment types and workload, as well as licensing and quality assurance mechanisms. All content is produced under the CC BY-SA 4.0 license, promoting openness, reusability, and co-creation. Pedagogical quality is ensured through peer review, compliance with EU standards, and continuous updates to maintain relevance and currency.

The XiA framework integrates cybersecurity not only as a technical competency but also from ethical and legal perspectives. It addresses, for example, the ethical use of artificial intelligence in clinical environments, emphasizing responsible decision-making and patient safety. MCLBs also promote transparency and privacy in data handling, ensuring that healthcare professionals understand the implications of data use, sharing, and

protection. Additionally, the framework supports compliance with European legislation, such as the AI Act and European Health Data Space (EHDS), highlighting the harmonization of digital health practices with legal standards. Through this multidimensional approach, the XiA framework positions cybersecurity as a cornerstone of responsible innovation and governance in healthcare.

In the context of XiA, Continuing Professional Development (CPD) emphasizes the relevance of professional roles—particularly in healthcare cybersecurity—as well as flexibility and modularity, allowing learners to select blocks that align with their career goals. Practical cybersecurity skills are essential for safeguarding digital healthcare environments. Learners are trained to implement security protocols that protect sensitive health data and ensure system integrity. They also gain expertise in managing audit trails and access control systems, which are critical for monitoring data usage and preventing unauthorized access. The framework includes guidance for the secure integration of healthcare IT systems, such as solutions compliant with the Health Level 7 Fast Healthcare Interoperability Resources (HL7, 2025) standard, to promote interoperability without compromising security. Additionally, learners are introduced to the management of cloud-based healthcare information systems, equipping them to use and protect modern, distributed healthcare infrastructures. These competencies are vital for maintaining the confidentiality, integrity, and availability of health data in increasingly complex and interconnected digital ecosystems.

3.4 Comparative Analysis of Cybersecurity Education Approaches

The XiA Framework, ManagiDiTH programme, and CyberSecPro project each contribute distinct yet complementary approaches to cybersecurity education in the healthcare sector. While all three initiatives aim to strengthen cybersecurity competencies among healthcare professionals, they differ in scope, pedagogical structure, and target audiences.

XiA Framework emphasizes modular microlearning through Micro-Content Learning Blocks (MCLBs), which are aligned with EQF levels 5–7 and support microcredentialing. Cybersecurity is integrated across multiple MCLB families, with a dedicated *Security & Privacy* family addressing GDPR, HIPAA, anonymization, and secure data exchange. XiA's strength lies in its flexibility and adaptability for continuous professional development, making it suitable for both clinical and technical staff seeking targeted upskilling as well as for system developers.

ManagiDiTH, on the other hand, offers a formal joint master's degree programme with a comprehensive curriculum that includes a dedicated 6 ECTS module on *Cybersecurity for Health Systems*. The programme integrates cybersecurity themes across various study units and emphasizes interdisciplinary learning, human-centric design, and alignment with NIST and ECSF frameworks. Its pedagogical model supports strategic thinking and leadership in digital health transformation, targeting professionals with diverse backgrounds in healthcare, ICT, and management.

CyberSecPro provides a sector-specific training portfolio and offers twelve thematic modules for cybersecurity education in the healthcare sector. These modules cover both foundational and advanced topics, including threat intelligence, penetration testing, digital forensics, and emerging technologies. CyberSecPro's approach is highly practical, featuring gamified learning, cyber range simulations, and alignment with ECSF competencies. It is designed for scalable implementation across academic and vocational settings, addressing identified skills gaps through hands-on, scenario-based training.

In summary, XiA provides a flexible microlearning infrastructure, ManagiDiTH offers a structured academic pathway with interdisciplinary depth, and CyberSecPro delivers targeted, practice-oriented training modules. Together, these initiatives form a robust ecosystem for cybersecurity education in healthcare, supporting lifelong learning, professional specialization, and systemic resilience.

4. Developing Micro-Content Learning Blocks for Cybersecurity Education

This section presents an example of how cybersecurity education in the healthcare sector could be approached in the future. The aim is to illustrate a pedagogical and structural model that supports the development of relevant competencies through modular and flexible learning solutions. By outlining practical implementation strategies, this section guides educators and curriculum designers seeking to enhance cybersecurity skills among healthcare professionals in a rapidly evolving digital environment.

4.1 Example Approach for Advancing Cybersecurity Education in Healthcare

The evolving demands of society challenge traditional conceptions of learning and the channels for acquiring knowledge. Individual characteristics and traits must be better acknowledged, and the European Union has

made this perspective a central objective of its learning strategies. As we know, levels of intelligence and understanding of the surrounding world vary among individuals. There is no universal model that works for everyone. Teachers and educational institutions must seize opportunities for flexible learning to respond to environmental changes and remain up to date.

European standardization is systematically monitored in Finland. The National Qualifications Framework (FiNQF) is based on the European Qualifications Framework (EQF). FiNQF describes the qualifications and competence structures of the national education system, covering, for example, general education, vocational education, and higher education. Competence structures are organized into eight levels based on the skills they require. The competencies for each level are defined in a government decree, and the descriptions correspond to EQF requirements. The Finnish Qualifications Framework is aligned with the European Higher Education Area (EHEA) framework (EDUFI, 2025). Curriculum design should be aligned with international standards such as the NIST Cybersecurity Framework (NIST, 2013) and the ECSF European Cybersecurity Skills Framework (ENISA, 2022), ensuring content relevance and transferability across EU member states.

Micro-learning content blocks (MCLBs) represent a modular and flexible approach to professional education, particularly well-suited for rapidly evolving fields such as healthcare cybersecurity. The pedagogical design of MCLBs should emphasize competency-based learning, and each block should begin with clearly defined and measurable objectives developed in accordance with Bloom's taxonomy. The curriculum should be structured in a modular format, enabling the organization of content into micro-courses that can be tailored to the needs of different stakeholders—such as healthcare professionals, IT managers, and system developers.

4.2 An Effective Pedagogical Approach for Cybersecurity Education

A sound pedagogical approach emphasizes experiential learning through case studies, simulations, and cyber range environments. It also incorporates a human-centered perspective, recognizing behavior, usability, and organizational culture as critical dimensions of cybersecurity. This is operationalized through the 3U model (User, Usage, Usability), ensuring that learners develop both technical proficiency and contextual understanding. Engagement and practical application should be fostered through interactive activities such as quizzes, simulations, and collaborative tasks. Both formative and summative assessments should be integrated into the learning experience to monitor progress and reinforce understanding.

Best practice recommends developing MCLBs into thematic families that address broad domains of digital health, such as interoperability, data protection, and cybersecurity. Each MCLB supports a broader learning pathway and can be combined into micro-courses designed to build specific competencies. These competencies are mapped to stakeholder roles, ensuring relevance and applicability in real healthcare settings.

4.3 Micro-credentials as Enablers of Modular Competence Recognition

Learners completing MCLBs or micro-courses may earn micro-credentials, serving as formal recognition of acquired skills. These credentials are aligned with EQF levels and can be issued by universities or other accredited bodies. A typical MCLB corresponds to approximately 0.1–0.2 ECTS credits, depending on workload, and can be aggregated into larger competence units over time.

Micro-credentials support modular recognition of competencies: learners can earn formal acknowledgments for completed modules (typically 0.1–5 ECTS), which can be stacked into broader qualifications, enabling personalized and scalable learning pathways. Micro-credentials enhance professional mobility and visibility, particularly in sectors such as healthcare, where regulatory requirements and technical expertise are critical. Content developers are encouraged to employ diverse formats—text, video, audio, and interactive media—to accommodate different learning styles and accessibility needs. All materials should adhere to open licensing principles to facilitate reuse and collaboration.

The micro-learning approach aligns well with cybersecurity frameworks. The European Cybersecurity Skills Framework (ECSF) supports the identification and structuring of role-based tasks, competencies, skills, and knowledge for European cybersecurity professionals. ECSF is an EU-level framework for defining and assessing competencies, endorsed by the European Commission in 2023 (ENISA 2022). It consolidates cybersecurity roles into 12 profiles, analyzed in terms of responsibilities, skills, synergies, and dependencies. ECSF provides a shared understanding of key roles, competencies, skills, and knowledge most frequently required in cybersecurity. It assists in identifying cybersecurity capabilities and supports the design of cybersecurity education.

Effective pedagogy in micro-learning content begins with clearly defined learning objectives that specify what learners should know or be able to do upon completing a block. Instructional design is grounded in learner-

centeredness, modularity, and competency-based education. These principles are essential for addressing the dynamic learning needs of healthcare professionals, particularly in the context of cybersecurity, where technological advancements demand continuous skill updates. Bloom's taxonomy is applied to formulate learning objectives across cognitive levels—from foundational understanding to advanced synthesis and evaluation. Curriculum design entails aligning learning objectives with teaching methods, assessment strategies, and learning resources. Table 1. illustrates and clarify the pedagogical and structural model supporting modular, competency-based cybersecurity education in healthcare.

The pedagogical framework integrates instructional quality, domain-specific content, and flexible delivery modes, strengthening cyber resilience among healthcare professionals. It promotes lifelong learning and professional mobility, contributing to the development of secure and sustainable digital healthcare systems across Europe.

Table 1: Modular-based Pedagogical and Structural Model for Cybersecurity Education

Model Layer	Key Elements	Pedagogical / Structural Function	XiA Framework Role	ManagiDiTH Master's Program Role	CyberSecPro Module Role
Policy & Standards Alignment	EQF, EHEA, FiNQF, NIST CSF, ENISA ECSF	Ensures international alignment, transferability, and recognition of competencies.	Provides organizational and process-level alignment templates.	Maps program learning outcomes to EQF level 7 and EHEA requirements.	Maps role-based skills and tasks to ECSF and NIST functions.
Pedagogical Principles	Competency-based learning, Bloom's taxonomy, 3U model, experiential learning.	Defines how learning objectives, activities, and assessments are designed.	Supports integration of human, organizational, and technical perspectives.	Implements learner-centered pedagogy and experiential projects.	Emphasizes applied learning through labs and simulations.
Structural Modularity	MCLBs, micro-courses, thematic families, learning pathways	Enables flexible, stackable, and reusable learning units.	Supplies reusable content patterns and case assets.	Curates MCLBs into degree-aligned micro-courses and pathways.	Provides ready-made modular training units.
Learning Design & Delivery	Case studies, cyber ranges, simulations, interactive activities.	Supports practical application and engagement.	Contributes cross-context case libraries.	Coordinates blended delivery and capstone projects.	Delivers role-based labs and scenario exercises.
Assessment Strategy	Formative and summative assessments, authentic tasks.	Measures progress and competency attainment.	Provides evaluation templates and usability metrics.	Defines program-level assessment rubrics.	Uses skills checklists and lab-based assessments.
Credentialing	Micro-credentials, ECTS stacking, digital badges.	Enables formal recognition and lifelong learning pathways.	Supports evidence packaging for micro-credentials.	Issues university-backed micro-credentials and degree credits.	Issues role-aligned micro-credentials.

5. Discussion

This paper has introduced a modular, interdisciplinary, and scalable model for cybersecurity education tailored to the healthcare sector. The model integrates three complementary European initiatives: the XiA Framework, the ManagiDiTH master's programme, and the CyberSecPro training modules. Together, these components form a comprehensive educational ecosystem that addresses the complex and evolving cybersecurity needs of healthcare professionals.

The XiA Framework contributes flexibility and accessibility through its Micro-Content Learning Blocks (MCLBs), which support just-in-time learning and microcredentialing. These blocks are particularly suitable for professionals who require targeted upskilling without committing to full degree programmes. The ManagiDiTH programme adds academic depth and strategic perspective, offering a formal master's degree with interdisciplinary content and a strong emphasis on human-centric cybersecurity. CyberSecPro complements these approaches with hands-on, scenario-based training modules that are aligned with European cybersecurity frameworks and designed to address real-world threats and skills gaps. By combining these strengths, the proposed model supports lifelong learning, professional mobility, and systemic resilience in healthcare cybersecurity. It enables learners to acquire both technical competencies and contextual awareness, fostering a

culture of security across clinical, administrative, and technical roles. The modular nature of the model makes it well-suited for integration into various educational contexts, including continuing professional development (CPD) programmes, vocational training, and higher education. Learners can pursue personalized learning journeys that align with their professional roles and career goals. The model also supports scalable deployment across EU member states, enhancing its relevance and reach.

Formal recognition of learning achievements is facilitated through microcredentials, typically ranging from 1 to 5 ECTS. These credentials validate acquired skills and contribute to employability and career advancement. However, successful implementation of the model requires institutional commitment to curriculum innovation, as well as active collaboration between educational institutions, healthcare providers, and cybersecurity experts.

Challenges may arise in maintaining the currency and relevance of content, especially in a rapidly evolving field like cybersecurity. Therefore, mechanisms for regular curriculum updates, quality assurance, and learner feedback are essential. On the other hand, modularity facilitates the maintenance of up-to-date content. Additionally, ensuring interoperability between different educational systems and credentialing frameworks across Europe will be critical for widespread adoption.

Future research should focus on empirical validation of the model through pilot implementations and longitudinal studies. Learner experience, satisfaction, and outcomes should be systematically evaluated to refine the pedagogical approach and enhance effectiveness. Moreover, expanding the curriculum to include emerging domains such as quantum-safe cryptography, explainable artificial intelligence, and digital ethics will ensure that the model remains responsive to future challenges.

6. Conclusion

In the context of the EU´s digital strategy the frameworks presented and related projects support the needs identified by the EU to harmonize the interconnection of IT skills needs, challenges created by artificial intelligence and education in the healthcare sector where public sector and private sectors actively cooperate. The rapidly evolving AI-assisted digital world of work environment also requires rapid response in education and understanding of professionals. The XIA framework with Micro-Content learning blocks is one example and one way to effectively meet local or regional ethical needs at a practical level, which the healthcare sector, and in particular patient safety, requires when developing common standardization in the sector.

Acknowledgements

This research was conducted within the framework of three EU-funded projects:

ManagiDiTH (Grant No. 101083896)

CyberSecPro (Grant No. 101083594)

XiA – Xpanding Innovative Alliance (Grant No. 101187650)

All projects are supported by the European Health and Digital Executive Agency (HADEA).

Ethics declaration: Ethical clearance was not required for the research.

AI declaration: Artificial intelligence (AI) was utilized to support language refinement, and structural coherence. AI-assisted tools were employed to analyze and integrate information from multiple EU-funded projects, ensuring consistency in terminology and alignment with pedagogical frameworks. While all conceptual contributions and interpretations remain the responsibility of the author.

References

Aljanabi, M. (2023) 'Safeguarding Connected Health: Leveraging Trustworthy AI Techniques to Harden Intrusion Detection Systems Against Data Poisoning Threats in IoMT Environments', *Babylonian Journal of Internet of Things*, 2023, pp. 31–37. Available at: https://doi.org/10.58496/BJIoT/2023/005.

Bowen, G.A. (2009) 'Document Analysis as a Qualitative Research Method', *Qualitative Research Journal*, 9(2), pp. 27–40. Available at: https://doi.org/10.3316/QRJ0902027.

CyberSecPro (2025) 'CyberSecPro'. Available at: https://www.cybersecpro-project.eu/ (Accessed: 9 October 2025).

EDUFI (2025) *Qualifications frameworks | Finnish National Agency for Education*. Available at: https://www.oph.fi/en/education-and-qualifications/qualifications-frameworks (Accessed: 1 December 2025).

ENISA (2022) *European Cybersecurity Skills Framework (ECSF) | ENISA*. Available at: https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf (Accessed: 1 December 2025).

European Parliament (2017) *C_2017189EN.01001501.xml*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2017_189_R_0003 (Accessed: 1 December 2025).

Ezeah, H.J. (2024) 'Big Data and Privacy with a focus on Statistical Approaches to Ensuring Data Confidentiality', *NEWPORT INTERNATIONAL JOURNAL OF CURRENT ISSUES IN ARTS AND MANAGEMENT*, 4(3), pp. 72–74. Available at: https://doi.org/10.59298/NIJCIAM/2024/4.3.7274.

Forood, A.M.K. *et al.* (2024) 'Advancements in health information technology and their role in enhancing cancer care: Innovations in early detection, treatment, and data privacy', *GSC Advanced Research and Reviews*, 21(1), pp. 228–241. Available at: https://doi.org/10.30574/gscarr.2024.21.1.0380.

Grobler, M., Gaire, R. and Nepal, S. (2021) 'User, Usage and Usability: Redefining Human Centric Cyber Security', *Frontiers in Big Data*, 4. Available at: https://doi.org/10.3389/fdata.2021.583723.

HL7 (2025) *Welcome to the HL7 FHIR Foundation*. Available at: https://www.fhir.org/ (Accessed: 1 December 2025).

Koutras, D. *et al.* (2024) *D3.3 CyberSecPro Portfolio of Cybersecurity Curricula Targeted to Health*. Available at: https://www.cybersecpro-project.eu/wp-content/uploads/2024/06/D3.3_CyberSecPro_Health_vFinal5_12_submitted.pdf (Accessed: 1 December 2025).

ManagiDiTH (2025) 'ManagiDiTH – Master of Managing Digital Transformation in the Health Sector'. Available at: https://managidith.eu/ (Accessed: 25 November 2025).

NIST (2013) 'Cybersecurity Framework', *NIST* [Preprint]. Available at: https://www.nist.gov/cyberframework (Accessed: 1 December 2025).

Priestman, W. *et al.* (2019) 'Phishing in healthcare organisations: threats, mitigation and approaches', *BMJ Health & Care Informatics*, 26(1). Available at: https://doi.org/10.1136/bmjhci-2019-100031.

Rajamäki, J. *et al.* (2024) 'Enhancing Cybersecurity Education for the Healthcare Sector: Fostering Interdisciplinary ManagiDiTH Approach', in *2024 IEEE Global Engineering Education Conference (EDUCON). 2024 IEEE Global Engineering Education Conference (EDUCON)*, pp. 1–7. Available at: https://doi.org/10.1109/EDUCON60312.2024.10578769.

Rajamäki, J., Nepal, A. and Chalkias, I. (2025) 'Implementing CTI Exchange: A Framework for the DYNAMO Project Pilot Phase', *European Conference on Knowledge Management*, 26(1), pp. 709–718. Available at: https://doi.org/10.34190/eckm.26.1.3780.

Rajamäki, J. and Postolache, O.A. (2025) 'Trialogical Learning and Academia-Industry Partnerships in "Sensors for Medical Instrumentation and Signal Processing" Curricular Unit of the ManagiDiTH Master's Program', in M.E. Auer and T. Rüütmann (eds) *Futureproofing Engineering Education for Global Responsibility*. Cham: Springer Nature Switzerland (Lecture Notes in Networks and Systems), pp. 157–168. Available at: https://doi.org/10.1007/978-3-031-85652-5_17.

Rathod, P. *et al.* (2023) 'D2.1 Cybersecurity Practical Skills Gaps in Europe: Market Demand and Analyse'.

Reeves, T. (2006) 'Design research from a technology perspective', in *Educational design research*. Routledge, pp. 64–78. Available at: https://www.taylorfrancis.com/chapters/edit/10.4324/9780203088364-13/design-research-technology-perspective-thomas-reeves (Accessed: 1 December 2025).

Tavares, A., Sousa, P. and Proença, R. (2024) 'Exploring the dynamics between artificial intelligence and cybersecurity in Healthcare', *ARIS2 - Advanced Research on Information Systems Security*, 4(1), pp. 20–34. Available at: https://doi.org/10.56394/aris2.v4i1.44.

Wang, F. and Hannafin, M.J. (2005) 'Design-based research and technology-enhanced learning environments', *Educational Technology Research and Development*, 53(4), pp. 5–23. Available at: https://doi.org/10.1007/BF02504682.

XiA (2025) 'XiA – Xpanding Innovative Alliance'. Available at: https://xia-project.iscte-iul.pt/ (Accessed: 12 November 2025).

Yin, R.K. (2018) *Case study research and applications: design and methods*. Sixth edition. Los Angeles London New Delhi Singapore Washington DC Melbourne: SAGE.

Zhang, J. and Zhang, Z. (2023) 'Ethics and governance of trustworthy medical artificial intelligence', *BMC Medical Informatics and Decision Making*, 23(1), p. 7. Available at: https://doi.org/10.1186/s12911-023-02103-9.

Zhou, Z. *et al.* (2024) 'A statistical approach to secure health care services from DDoS attacks during COVID-19 pandemic', *Neural Computing and Applications*, 36(1), pp. 1–14. Available at: https://doi.org/10.1007/s00521-021-06389-6.