From Compliance to Practice: Persona-based Microlearning Model for Healthcare Cybersecurity

Jenna Hemtman, Ronja Salonen, Klaus Aalto, Andrej Ylinen, Aleksi Hakkarainen, Joonas Ilomäki, Idil Hussein, Kristian Virta and Jyri Rajamäki
Laurea University of Applied Sciences, Espoo, Finland

jenna.hemtman@student.laurea.fi
ronja.salonen@student.laurea.fi
klaus.aalto@student.laurea.fi
andrej.ylinen@student.laurea.fi
aleksi.hakkarainen@student.laurea.fi
joonas.ilomaki@student.laurea.fi
idil.hussein@student.laurea.fi
kristian.virta@student.laurea.fi
jyri.rajamaki@laurea.fi

Abstract: Healthcare organisations across Europe are simultaneously facing increasing cybersecurity threats and stringent regulatory requirements introduced by the European Health Data Space (EHDS). While compliance frameworks define necessary technical and legal standards, they do not sufficiently address how healthcare professionals and IT managers translate these requirements into everyday practice. This paper presents a pedagogical model that integrates persona-based design with microlearning to bridge the gap between compliance and practice. The approach combines two complementary learner perspectives: (1) IT managers responsible for EHDS compliance in resource-constrained healthcare settings, and (2) healthcare professionals with low-to-medium digital literacy operating in high-pressure clinical environments. The proposed solution is a persona-based microlearning model built on Micro-Content Learning Blocks (MCLBs), enabling work-integrated, role-specific learning. The persona-based microlearning model emphasises practical outputs such as compliance documentation, risk recognition, and secure decision-making rather than theoretical knowledge acquisition. Initial design results suggest that persona-based microlearning can reduce cognitive load, improve behavioural relevance, and support scalable cybersecurity education in healthcare.

Keywords: EHDS, Cybersecurity Education, Microlearning, Personas, Healthcare, Digital Literacy, Work-Integrated Learning

1. Introduction

Healthcare systems are undergoing rapid digital transformation, increasing both opportunities for data-driven care and exposure to cybersecurity risks (Ogbodo et al., 2025). At the same time, the European Health Data Space (EHDS) introduces comprehensive requirements for interoperability, data governance, and cybersecurity across EU member states (Gyrard et al., 2025).

The Xpanding Innovative Alliance (XiA, 2026) project is a European education and development initiative aimed at supporting higher education institutions and workplaces in preparing for digital transformation, particularly the competencies required by EHDS. The project focuses on developing flexible, work-integrated learning solutions grounded in microlearning, personalization, and competence-based approaches. Its core objective is to bridge the gap between regulatory requirements and practical capabilities, especially in the domains of cybersecurity and digital skills in healthcare. This study has been conducted within the XiA project and builds on its pedagogical principles, including the use of Micro-Content Learning Blocks (MCLBs) and persona-based learning design. A fundamental challenge lies in translating EHDS requirements into everyday practice. Small healthcare organisations face significant resource constraints in implementing compliance, while frontline healthcare professionals must make secure decisions in fast-paced and high-pressure environments.

Although prior research has demonstrated the effectiveness of microlearning in time-constrained professional environments (Monib et al., 2024) and highlighted the benefits of persona-based approaches in cybersecurity education (Ki-Aries & Faily, 2017), a clear gap remains in the literature. Existing approaches tend to address either compliance-level competencies (e.g., legal, technical, and organisational requirements) or user-level awareness and behaviour (Nma, 2023), but rarely integrate these into a unified pedagogical framework. Furthermore, much cybersecurity training remains abstract and fails to translate into behavioural change in real-world work situations, particularly in high-pressure domains such as healthcare.

This study addresses this gap by proposing a persona-based microlearning model that bridges compliance and practice. In this study, persona-based microlearning refers to short, role-specific learning interventions designed around representative learner personas. Rather than providing generic cybersecurity training, the approach tailors scenarios, decisions, examples, and expected outputs to the needs of specific user groups such as IT managers and frontline healthcare professionals. The personas serve as design anchors that ensure contextual relevance while maintaining the brevity characteristic of microlearning. In this study, two representative personas are utilised: Anna, an IT manager responsible for EHDS compliance in a resource-constrained healthcare organisation, and Maria, a healthcare professional working in a time-constrained clinical environment.

The theoretical contribution of this paper is threefold: (1) An integrated dual-layer learning framework that connects organisational compliance competencies with individual-level cybersecurity practices. (2) An operationalisation of persona-based microlearning, suggesting how heterogeneous learner needs (e.g., IT managers vs. healthcare staff) can be systematically embedded into a scalable learning architecture. (3) A practice-oriented pedagogical approach that shifts the focus from knowledge acquisition to action, emphasising real-world tasks, decision-making, and work-based outputs. Together, these contributions extend the literature on cybersecurity education and microlearning by offering a unified model that links regulatory compliance with everyday secure behaviour in healthcare contexts.

The research question guiding this study is: “How can complex cybersecurity and regulatory requirements be transformed into practical, persona-based learning experiences in healthcare that support both compliance and behavioural change?” To address this, the paper proposes a persona-based microlearning model that integrates compliance-oriented learning (targeting IT leadership) with practice-oriented learning (targeting healthcare professionals), aiming to move from compliance to actionable, secure practice.

2. Background and Related Work

2.1 EHDS and Compliance Challenges

The European Health Data Space (EHDS) aims to establish a secure and interoperable framework for the exchange and use of health data across the European Union. Its objectives include improving data accessibility, supporting continuity of care across borders, and enabling the secondary use of health data for research and innovation (European Commission, 2025; European Parliament, 2025).

The implementation of EHDS places new demands on healthcare organisations. In addition to meeting regulatory requirements, organisations must ensure secure data governance, interoperability, and cybersecurity across increasingly digital healthcare environments. These requirements are particularly relevant in contexts involving electronic health records, cross-border healthcare services, and connected medical technologies.

For many healthcare organisations, especially those with limited resources, translating EHDS requirements into operational practices presents a significant challenge. Compliance requires not only technical and organisational measures but also the ability of healthcare professionals and managers to make secure decisions in their daily work. This highlights the need for learning approaches that connect regulatory requirements with practical workplace behaviour and competence development.

2.2 Cybersecurity Education in Healthcare

Cybersecurity education has become a critical component of organizational resilience, particularly in environments where sensitive patient data is handled through interconnected digital systems. Although technical safeguards continue to evolve, the human factor remains the most significant vulnerability; industry reports indicate that a vast majority of data breaches involve human error or human-related risk factors (Mimecast, 2026). In healthcare, where decisions are made under intense pressure, the consequences of these errors are increasingly costly. The global average cost of a data breach has reached 4.1 million euros, with the healthcare sector consistently ranking as the most expensive industry for the 15th consecutive year. Despite the rise of automated security, 97% of organizations reporting incidents lacked proper access controls, and 63% operated without clear AI governance policies (IBM 2025). The core of this study lies in the urgent need to develop solutions that move beyond merely teaching rules to effectively transforming behaviour within the demanding context of clinical work. This view is also supported by earlier healthcare research, which found that

cybersecurity incidents in healthcare organizations are linked to low staff awareness and highlighted the importance of continuous security awareness training programmes (Gioulekas, et al., 2022).

2.3 Limitations of Generic Training

General cybersecurity training can improve awareness and basic knowledge, but its effect on actual behaviour is often more limited than its effect on attitudes and understanding (Prümmer et al., 2025). In healthcare settings, this is a clear weakness, because staff need to make secure choices in real situations and often under time pressure. Research has also indicated that many security education approaches remain too compliance-driven and are not always closely connected to employees' actual work context (Williams et al., 2024). In addition, NIST (2024) emphasises that cybersecurity learning should be adapted to different audiences, roles and skill gaps rather than relying on one general format for everyone.

2.4 User-Centered and Microlearning in Cybersecurity Education

A user-centred and targeted approach provides a strong foundation for cybersecurity education, as it takes into account how individuals learn and apply knowledge in real-world contexts. Rather than assuming that a single training format is suitable for all users, this approach allows learning to be adapted to different roles, needs, and levels of expertise within healthcare organisations (Ki-Aries & Faily, 2017; NIST, 2024). This perspective is supported by research on persona-centred cybersecurity awareness, which emphasises the importance of understanding distinct user groups and their specific capability gaps. By incorporating personas into learning design, it is possible to create training that is directly relevant to learners' professional roles and work environments (Ki-Aries & Faily, 2017). Furthermore, this aligns with recommendations from standards bodies such as NIST, which highlight the need to tailor cybersecurity education to different audiences rather than relying on generic training models (NIST, 2024).

Microlearning further strengthens this approach by enabling short, focused learning experiences that can be integrated into everyday workflows. In time-constrained environments such as healthcare, microlearning allows professionals to engage with training in manageable segments without disrupting their primary responsibilities (Buchem & Hamelmann, 2010). This makes it particularly suitable for continuous professional development and rapid upskilling in contexts characterised by high workload and limited training time. The integration of persona-based design and microlearning creates a flexible and scalable educational model. Learning content can be structured into modular units that align with specific competencies while remaining adaptable to different contexts and learner groups.

Engagement can be enhanced through the use of gamification and scenario-based learning techniques (Carreiro et al., 2024). These methods have been shown to improve learner motivation, participation, and retention in cybersecurity training contexts (Bitrián et al., 2024; Carreiro et al., 2024). By encouraging active participation, reflection, and repeated practice, such approaches support the development of practical cybersecurity skills. Overall, the combination of user-centred design, microlearning structures, and interactive elements enables cybersecurity education to move beyond awareness-building towards supporting meaningful behavioural change in real work situations (Prümmer et al., 2025).

Healthcare cybersecurity involves heterogeneous learner groups with substantially different responsibilities, digital competencies, and decision-making contexts. A generic microlearning approach risks presenting irrelevant content to many users. Persona-based design is therefore used to increase contextual relevance, reduce unnecessary cognitive load, and support the transfer of learning into daily work practices.

2.5 The XiA Framework

The Xpanding Innovative Alliance (XiA) Framework provides the pedagogical foundation for this study. The framework has been developed to support digital transformation in healthcare through modular, flexible, and work-integrated learning. Central to the framework is the concept of Micro-Content Learning Blocks (MCLBs), which are short, outcome-oriented learning units aligned with the European Qualifications Framework (EQF) and designed to support micro-credentialing and continuous professional development.

Within XiA, learning is structured around clearly defined outcomes, practical workplace relevance, and competence development. MCLBs can be combined into larger learning pathways while remaining sufficiently compact to fit the needs of working professionals. This makes the approach particularly suitable for domains

such as healthcare cybersecurity, where competencies must be continuously updated without disrupting everyday work activities.

The XiA framework further emphasises learner-centred design and the alignment of learning activities, assessment, and professional tasks. Rather than treating cybersecurity solely as a technical issue, the framework supports role-specific competence development that integrates technical, organisational, legal, and ethical perspectives.

In this study, XiA serves as the pedagogical basis for developing a persona-based microlearning model for healthcare cybersecurity. The proposed model extends XiA principles by incorporating learner personas and a dual-layer structure that addresses both organisational compliance requirements and frontline healthcare practice.

3. Research Approach

This study adopts Hevner's et al. (2004) design science approach to develop and conceptualise a persona-based microlearning model for healthcare cybersecurity. The approach is grounded in the pedagogical principles and development processes defined within the XiA Pedagogy Handbook, which provides a structured and practice-oriented framework for designing MCLBs. The research focuses on translating these pedagogical principles into a domain-specific application that addresses the dual challenge of regulatory compliance and behavioural change in healthcare cybersecurity. Rather than evaluating an existing system, the study aims to design and articulate a pedagogical solution that can later be implemented and empirically validated.

The research approach combines design science methodology with established pedagogical principles from the XiA framework to develop a scalable and practice-oriented model for healthcare cybersecurity education. The approach ensures methodological rigor through structured design processes while maintaining practical relevance through persona-based and work-integrated learning design.

At the core of the approach is the MCLB concept, functioning as modular, outcome-oriented learning units. Each MCLB is designed to target a clearly defined learning outcome and represents a self-contained unit of learning that can also be combined into larger structures such as micro-courses and micro-credentials. The modular nature of MCLBs enables flexibility, scalability, and personalization, supporting continuous professional development in dynamic environments such as healthcare. The development process follows a structured and iterative design logic, as defined in the XiA framework. The process begins with the specification of learning outcomes aligned with European Qualifications Framework (EQF) levels and formulated using action-oriented verbs derived from Bloom's taxonomy. These outcomes guide the design of all subsequent elements, ensuring coherence between intended competencies, learning activities, and assessment.

Following the outcome definition, the design process involves the creation of learning activities that support active engagement and practical application. In line with the XiA pedagogical approach, activities are structured into short sequences combining content exposure (e.g., text or video) with immediate application (e.g., case-based tasks or decision-making exercises). This structure promotes active learning and reduces cognitive overload by limiting content scope and focusing on essential concepts.

A key methodological principle guiding this study is the emphasis on learner-centred and outcome-oriented design. The development of learning content is informed by learner personas representing distinct user groups, such as IT managers and healthcare professionals. These roles provide contextual grounding for the design process, ensuring that learning solutions are aligned with real-world tasks, constraints, and professional environments. Assessment is integrated as an inherent component of each learning unit, rather than as a separate evaluative phase. The XiA model emphasises practice-oriented assessment, where learners demonstrate competence through realistic tasks aligned with defined learning outcomes. Assessment is typically implemented using simplified pass/fail criteria, reflecting minimum acceptable professional performance rather than detailed grading. This approach supports transparency and reinforces the connection between learning and practical competence.

The design process is further supported by considerations related to alignment, usability, and quality assurance. All learning components—outcomes, activities, and assessment—must be coherently aligned to ensure pedagogical effectiveness. In addition, accessibility and usability principles, including compliance with WCAG guidelines, are incorporated to ensure that learning materials are inclusive and adaptable across different user contexts.

Finally, the research approach acknowledges the iterative nature of microlearning design. The persona-based microlearning model developed in this study represents an initial conceptual artefact that can be refined through future implementation, feedback, and empirical validation. This aligns with the XiA framework's emphasis on continuous improvement and adaptability in educational design.

4. Persona-based Microlearning Model

Figure 1 presents the overall structure of the Persona-based microlearning model. The model is grounded in two representative learner personas: Anna represents an IT manager in a resource-constrained healthcare organisation responsible for EHDS compliance, whereas Maria represents a frontline healthcare professional working in a time-constrained clinical environment. Based on these personas, the model provides two parallel learning pathways that address organisational compliance and everyday cybersecurity practice. The personas are design artefacts rather than real individuals and are used to ensure the contextual relevance of learning activities, scenarios, and assessments.

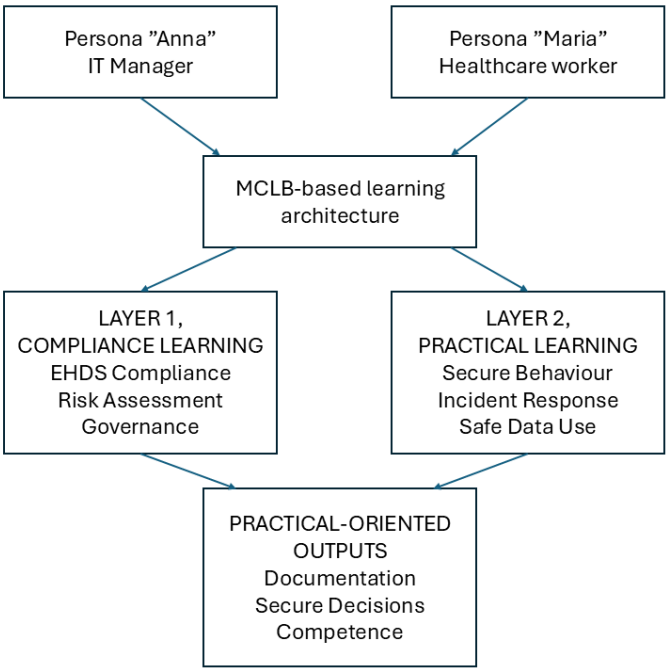


Figure 1: Overview of the Persona-based Microlearning Model for Healthcare Cybersecurity

4.1 Pedagogical Framework

The proposed solution defines a structured microlearning-based training system tailored to healthcare cybersecurity. Rather than representing a single digital platform, the persona-based microlearning model functions as a design blueprint that specifies how learning content is structured, delivered, and assessed.

The model is implemented through MCLBs, which serve as modular, outcome-oriented learning units. Each MCLB is designed to be completed within a short time frame of approximately 15 to 45 minutes, making it suitable for integration into demanding healthcare workflows. The design ensures that learning units are mobile-accessible and minimise cognitive load, thereby enabling learners to engage with content without interrupting their primary professional responsibilities.

In line with the XiA framework, the overall workload corresponds to approximately one ECTS credit, which equals around 26 hours of learning distributed across multiple microlearning units. Importantly, the model prioritises the production of practical outputs, such as compliance documentation, risk analyses, and decision-making artefacts, rather than focusing solely on theoretical knowledge acquisition.

4.2 Dual-Layer Learning Design

The Persona-based microlearning events incorporate case- and scenario-based elements, but differ from traditional case-based learning by being intentionally condensed into microlearning units, personalised through

learner personas, and directly linked to specific workplace outputs and competencies. A key innovation of the Persona-based microlearning model is its dual-layer learning design, which integrates two complementary perspectives within a unified pedagogical structure. This approach ensures that both organisational compliance requirements and individual-level behaviour are addressed simultaneously. The two layers are parallel persona-guided learning pathways rather than sequential stages.

4.2.1 Layer 1: Compliance-Oriented Learning (IT Perspective)

The first layer is designed for IT managers and decision-makers who are responsible for implementing EHDS compliance in healthcare organisations. The learning content focuses on translating regulatory requirements into actionable organisational practices. In this layer, learners engage with topics such as legal responsibilities and vendor management under EHDS, technical interoperability standards including EEHRxF and xShare, as well as cybersecurity audit trails and ethical data governance. The learning outcomes are operationalised through the creation of concrete artefacts. For example, learners are required to develop vendor requirement lists based on risk assessments, produce technical compliance roadmaps tailored to their organisational context, and generate risk assessment and audit documentation aligned with regulatory requirements. These outputs are designed to be directly applicable in the workplace, thereby supporting real compliance processes rather than remaining at a conceptual level.

4.2.2 Layer 2: Practice-Oriented Learning (Clinical Perspective)

The second layer targets healthcare professionals who operate in clinical and field environments. Its primary objective is to support secure behaviour and decision-making in real-world situations, particularly under conditions of time pressure and uncertainty. The content in this layer focuses on practical cybersecurity-related activities, including the secure use of mobile devices and digital tools, the safe handling and sharing of patient data, the recognition and reporting of cybersecurity incidents, and decision-making in high-risk or ambiguous situations. Learning is implemented through scenario-based microlearning, where learners interact with realistic situations that mirror their daily work tasks. These scenarios require the learner to make decisions, reflect on possible outcomes, and apply appropriate cybersecurity practices. In addition, the persona-based microlearning model incorporates gamified elements and reflective activities, which serve to enhance engagement and reinforce behavioural learning. The emphasis of this layer is on enabling immediate applicability of knowledge in practice, thereby strengthening the connection between learning and professional performance.

4.3 Learning Mechanisms

The persona-based microlearning model applies a consistent and repeatable learning loop, which structures each MCLB. Each learning process begins with a diagnostic pre-check, through which learners evaluate their existing knowledge and identify areas where learning is required. This mechanism allows learners to skip content they have already mastered, thereby improving efficiency and personalisation. Following this, the learner engages with a microlearning intervention that delivers content in a short and focused format. This content may include short videos, concise textual explanations, or illustrative examples, each targeting a single clearly defined learning objective.

The learning process culminates in a work-based task or decision-making activity, in which the learner applies the acquired knowledge in a practical context. These tasks are typically case-based or scenario-driven and require the learner to analyse situations, make informed decisions, or produce concrete outputs relevant to their professional role. This structured loop ensures that learning remains active, personalised, and directly applicable to real-world tasks. Assessment is fully integrated into the learning process and focuses on demonstrating competence rather than recalling information. Learners are evaluated based on their ability to perform relevant tasks, make appropriate decisions, and produce valid outputs.

Within this persona-based microlearning model, the role of the instructor shifts significantly compared to traditional teaching approaches. Instead of acting primarily as a content provider, the instructor functions as a facilitator who supports learning in context, provides targeted feedback, and ensures the quality and relevance of learning materials.

5. Resulting Pedagogical Model

At the current stage of the research, the primary result is the development of a conceptual persona-based microlearning model for healthcare cybersecurity. The model was designed as a pedagogical artefact that addresses the identified gap between regulatory compliance requirements and practical cybersecurity behaviour in healthcare environments.

The resulting artefact combines three key design elements. First, it applies microlearning principles through the use of Micro-Content Learning Blocks (MCLBs), enabling learning to be integrated into busy healthcare workflows. Second, it incorporates persona-based learning design to address the differing needs and responsibilities of healthcare professionals and IT managers. Third, it links learning activities directly to workplace-relevant tasks, decisions, and outputs rather than focusing primarily on theoretical knowledge acquisition.

The persona-based microlearning model operationalises these principles through a dual-layer structure. One learning pathway addresses organisational cybersecurity and EHDS compliance from the perspective of IT managers and decision-makers, while the other focuses on secure day-to-day practices among healthcare professionals. By connecting these perspectives within a single pedagogical framework, the model seeks to bridge the gap between organisational requirements and frontline behaviour.

As the study is currently conceptual and design-oriented, the results should be interpreted as a theoretically grounded design proposal rather than an empirically validated solution. Nevertheless, the artefact demonstrates how persona-based microlearning can be structured to support role-specific learning, practical competence development, and workplace integration in healthcare cybersecurity education. The proposed model therefore provides a foundation for future pilot implementations and empirical evaluation.

6. Discussion

A central premise of this study is the need to move beyond compliance-driven approaches towards practice-oriented cybersecurity learning. Prior research suggests that increasing awareness alone does not necessarily lead to behavioural change, particularly in high-pressure environments such as healthcare.

The proposed model addresses this limitation by embedding compliance requirements directly into work-related decision-making processes and tangible outputs. In doing so, it transforms cybersecurity learning from an abstract requirement into an integral part of everyday professional practice.

6.1 Theoretical Contributions

This research advances existing literature by introducing a persona-based microlearning model that integrates organisational-level compliance competencies with individual-level behaviour within a single pedagogical structure. While previous studies have treated these dimensions separately, this work suggests their interdependence and proposes a mechanism for aligning them.

The study contributes by providing a concrete model for combining persona-based design with microlearning. It suggests how different user groups—with varying roles, capabilities, and constraints—can be systematically addressed within a unified and scalable learning framework.

The proposed approach shifts the focus of cybersecurity education from knowledge acquisition to actionable competence. By emphasising work-based outputs, decision-making, and reflection, the persona-based microlearning model aligns with “learning-by-doing” paradigms and addresses the documented gap between awareness and behavioural change.

The innovation of the persona-based microlearning model does not lie in microlearning, roles, scenario-based learning, or compliance training individually. Rather, its novelty emerges from integrating these elements into a unified architecture that simultaneously addresses organisational compliance requirements and frontline behavioural practice within the context of EHDS implementation.

6.2 Practical Implications

The Persona-based microlearning model has several important practical implications for healthcare organisations seeking to improve cybersecurity readiness while operating under resource constraints. First, the use of microlearning enables the integration of training into everyday workflows, allowing professionals to

engage with learning content within limited time windows without disrupting clinical or administrative duties. This is particularly critical in healthcare environments, where time pressure and workload intensity often hinder participation in traditional training programmes.

Second, the persona-based design ensures that learning content is aligned with the specific roles, responsibilities, and competence levels of different user groups. By tailoring learning experiences to the needs of both IT managers and frontline healthcare professionals, the persona-based microlearning model increases relevance and supports more effective knowledge transfer into practice. This role-specific alignment also reduces unnecessary cognitive load, as learners are not required to engage with irrelevant or overly technical material.

Third, the model emphasises the production of practical outputs, such as risk assessments, compliance documents, and action plans, which can be directly applied within the organisation. This approach enhances the immediate usability of learning outcomes and strengthens the connection between training and operational improvement.

Finally, the modular and scalable nature of the framework allows it to be extended to additional roles, organisations, and contexts. As such, the persona-based microlearning model provides a flexible foundation for developing organisation-wide cybersecurity education programmes that support both compliance with EHDS requirements and the development of secure everyday practices.

6.3 Limitations and Future Research

Despite its contributions, this study has several limitations that must be considered when interpreting the findings. First, the Persona-based microlearning model is based on a limited number of personas, which may not fully capture the diversity of roles, organisational structures, and national healthcare systems across the European context. As a result, the generalisability of the model remains constrained. Second, the study is currently conceptual and design-oriented, and no empirical validation has yet been conducted. The absence of pilot implementations and user testing means that the effectiveness of the model in real-world settings has not been systematically evaluated. Third, the scope of the pedagogical design is intentionally limited in order to maintain feasibility and focus. Consequently, certain aspects of EHDS compliance and broader cybersecurity competencies are not comprehensively addressed within the current model. These limitations highlight the need for further research and iterative development to validate, refine, and extend the proposed approach.

Future research should focus on validating and extending the Persona-based microlearning model through empirical investigation. A key priority is the implementation of pilot studies in healthcare organisations to assess the usability, effectiveness, and acceptance of the model among different user groups. Such studies would provide valuable insights into how the model performs in real-world environments and how it can be adapted to specific organisational contexts. In addition, further research is needed to evaluate the impact of the model on behavioural change. This includes the development of appropriate metrics and evaluation frameworks to measure improvements in secure practices, decision-making, and overall cybersecurity culture within healthcare organisations. Another important direction for future work is the expansion of the model to include additional professional roles, thereby increasing its applicability and scalability across diverse healthcare settings. This may also involve adapting the model to different national regulatory environments and organisational structures. Finally, the technological implementation of the persona-based microlearning model as a digital learning platform represents a critical next step. Future research should explore how the principles outlined in this study can be operationalised through user-friendly, accessible, and interoperable learning systems that support continuous, work-integrated cybersecurity education.

7. Conclusion

This paper presents a novel approach to healthcare cybersecurity education by integrating EHDS compliance requirements with persona-based microlearning. By combining IT-level compliance training with frontline practice-oriented learning, the persona-based microlearning model addresses both structural and human dimensions of cybersecurity. The results suggest that persona-based microlearning can effectively bridge the gap between compliance and practice, offering a scalable and adaptable solution for healthcare organisations facing increasing regulatory and cybersecurity demands.

Ethics Declaration

Ethical clearance was not required.

AI Declaration

Artificial intelligence was utilized in the writing process to support literature review synthesis, facilitate comparative analysis between findings and previous research, and assist in the formulation and translation of academic text. AI tools such as Keenious and Copilot enabled efficient information retrieval, structured drafting, and linguistic refinement, thereby enhancing the clarity, coherence, and overall quality of the manuscript. While all conceptual contributions and interpretations remain the responsibility of the authors.

Acknowledgements

This work was supported by the European Union under Grant Agreement No. 101187650 (XiA – Xpanding Innovative Alliance). Views and opinions expressed are, however, those of the authors only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

References

Bitrián, P., Buil, I., Catalán, S. & Merli, D. 2024. *Gamification in workforce training: Improving employees' self-efficacy and information security and data protection behaviours.* Journal of Business Research, 179, 114685. https://doi.org/10.1016/j.jbusres.2024.114685

Buchem, I., and Hamelmann, H. (2010). Microlearning: a strategy for ongoing professional development. *eLearning Papers*, *21*(7), 1-15.

Carreiro, A., Silva, C. & Antunes, M. 2024. *The use of gamification on cybersecurity awareness of healthcare professionals.* ScienceDirect. https://www.sciencedirect.com/science/article/pii/S1877050924014455

European Commission (2025) *My rights over my health data - Public Health - European Commission*. Available at: https://health.ec.europa.eu/ehealth-digital-health-and-care/my-rights-over-my-health-data_en (Accessed: 11 November 2025).

European Parliament (2025) 'Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (Text with EEA relevance)'.

Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., Georgiadou, A., Michalitsi- Psarrou, A., Doukas, G., Kontoulis, M., Nikoloudakis, Y., Marin, S., Cabecinha, R. and Ntanos, C. 2022. *A cybersecurity culture survey targeting healthcare critical infrastructures.* Healthcare, 10 (2), 327. https://doi.org/10.3390/healthcare10020327

Gyrard, A. et al. (2025). Lessons Learned From European Health Data Projects With Cancer Use Cases: Implementation of Health Standards and Internet of Things Semantic Interoperability, Journal of Medical Internet Research, 27, pp. e66273. https://doi.org/10.2196/66273

Hevner, A. R., March, S. T., Park, J., and Ram, S. (2004). Design science in information systems research. *MIS quarterly*, *28*(1), 75-106.

IBM 2025. *Cost of a Data Breach Report 2025.* Accessed 12 March 2026. https://www.ibm.com/reports/data-breach/

Ki-Aries, D. and Faily, S. (2017). Persona-centred information security awareness. Computers & Security, 70, 663-674. https://doi.org/10.1016/j.cose.2017.08.001

Mimecast 2026. *The State of Human Risk 2026.* https://www.mimecast.com/resources/ebooks/state-of-human-risk/

Monib, W., Qazi, A. and Apong, R. (2024). Microlearning beyond boundaries: A systematic review and a novel framework for improving learning outcomes, Heliyon, Vol. 11, Iss. 2 e41413. https://doi.org/10.1016/j.heliyon.2024.e41413

NIST 2024. *Building a Cybersecurity and Privacy Learning Program.* NIST Special Publication 800-50r1.

Nma, J. 2023. *Safe and sound: Strengthening cybersecurity in healthcare through robust staff educational programs.* https://journals.sagepub.com/doi/10.1177/08404704231194577

Ogbodo, D. C., Awan, I.-U., Cullen, A., & Zahrah, F. (2025). From Regulation to Reality: A Framework to Bridge the Gap in Digital Health Data Protection. *Electronics*, *14*(13), p. e2629. https://doi.org/10.3390/electronics14132629

Prümmer, J., van Steen, T. and van den Berg, B. 2025. *Assessing the effect of cybersecurity training on end-users: A meta-analysis.* Computers & Security, 150, 104206. https://doi.org/10.1016/j.cose.2024.104206

XiA (2026). Xpanding Innovative Alliance. https://xia-project.iscte-iul.pt/

Williams, J. A., Zafar, H. and Gupta, S. 2024. *Fortifying healthcare: An action research approach to developing an effective SETA program.* Computers & Security, 138, 103655. https://doi.org/10.1016/j.cose.2023.103655