The Current Landscape of Cybersecurity Training in CAHIIM Accredited Programs

Huanmei Wu
Health Services Administration and Policy
Temple University College of Public Health
Philadelphia, PA, USA
Huanmei.Wu@Temple.edu

Mukesh Kumar Patel
Health Services Administration and Policy
Temple University College of Public Health
Philadelphia, PA, USA
mukesh.kumar.patel@temple.edu

Chiu C Tan
Computer and Information Science
College of Science and Technology
Philadelphia, PA, USA
chiu.tan@templee.edu

***Abstract*— Cybersecurity training for health professionals is important for different stakeholders in healthcare. This project aims to shed light on the current landscapes of cybersecurity training in CAHIIM-accredited programs in Health information management (HIM) and health informatics using natural language processing (NLP). The in-depth analysis focuses on the course contents, academic degrees offered, and the themes of these courses, such as security, ethics, and regulations, as well as the geographical distribution of institutions offering these programs. The research identifies trends in cybersecurity education within healthcare, emphasizing the integration of privacy and security measures in academic programs. It aims to shed light on the diversity and quality of cybersecurity training in HIM and health informatics programs, contributing to the development of standardized training frameworks and informing policy and educational strategy within the field.**

Keywords—cybersecurity, privacy, ethics, regulations, security

I. Introduction

The field of health informatics is rapidly advancing and playing an increasingly important role in healthcare by emphasizing interprofessional education [1]. Cybersecurity education in health informatics is crucial for healthcare professionals to secure our cyberinfrastructure, utilize health information systems safely, and enhance overall patient care [2-6]. The healthcare system faces specific cybersecurity challenges such as password reuse and outdated software, posing risks to healthcare infrastructure [7-11]. With the increasing integration of advanced intelligent technologies into healthcare, there is a growing demand for cybersecurity education for healthcare workers [12-13].

Most research on healthcare security training has focused on specific cybersecurity topics in healthcare, such as the effectiveness of phishing training, password practices, or the security of mobile devices [14-15]. Unlike these studies, our project focuses on broader cybersecurity education within academic programs, which encompasses general principles rather than specific topics. Research related to our work has explored cybersecurity curricula for healthcare professionals [16-18]. For example, Waddell recommended adopting methods from fields like aviation safety for delivering cybersecurity training topics. Swede et al. proposed a curriculum emphasizing regulatory compliance [19-20]. In contrast, our paper focuses on existing cybersecurity training in an academic setting.

II. Data and Methods

A. Degree Program List

We are examining academic programs in HIM and health informatics (HI) that are accredited by the Commission on Accreditation for Health Informatics and Information Management Education (CAHIIM) [21]. Our focus is on three types of programs: the Baccalaureate Degree in Health Information Management (BSHIM), the Master's Degree in Health Information Management (MSHIM), and the Master's Degree in Health Informatics (MSHI). This selection encompasses 116 programs across 97 institutions.

B. Data Acquisition and NLTK Text Processing

For each accredited program, the program course titles and descriptions (a short introduction of a specific course) are downloaded from the corresponding websites. The course title and description are searched with keywords for "cybersecurity,", "security," "privacy," "safety," and "risk". Those courses with the keywords (55 courses) are selected and further processed using the Natural Language Toolkit (NLTK).

First, the course descriptions are tokenized into words using the *word_tokenize()* method. Second, the NLTK stop words, which are common words such as "the," "is," or "and," are filtered out to focus on more meaningful words in the course descriptions. Third, the filtered words are further reduced to their root form (also known as the stem) using the NLTK stemming method, *porter_stemmer.stem()*. Next, the NLTK lemmatizing method *lemmatizer.lemmatize()* is applied to provide more context-aware words. After this processes, different cybersecurity terms, such as "Cyber Security" or "Cyber-Security" will be "cybersecurity." Last, the reduced root-based words in a course description are grouped into meaningful chunks for context based analysis.

C. Cybersecurity-related Analyses on Courses

Table 1 outlines the top three major themes related to cybersecurity that align with our research interests based on ChatGPT. Input from experts in cybersecurity and healthcare was used to identify keywords for each theme, which are listed in Table 1. Courses are categorized into one or more themes, and their details—including the associated programs, areas (HIM or HI), degrees (BS or MS), institutions, and geographical locations of the institutions—are documented accordingly.

III. Results

The majority of the CAHIIM-accredited programs focuses on HIM at the baccalaureate level. Some universities offer both undergraduate and graduate programs. Online programs are notably more prevalent than in-person options. Regarding security curriculum, 45 out of 116 programs (39%) from 36 out of 97 institutions (37%) offer courses on security and privacy. This includes 22 out of 73 BSHIM programs (30%), 7 out of 15 MSHIM programs (47%), and 16 out of 28 MSHI programs (57%). The results show that graduate programs, particularly MSHI programs, offer more courses on security-related topics.

The locations of the home institutes that offer security-related courses are geocoded using OpenStreetMap's geocoding service, specifically the *geopy.geocoders.Nominatim* class. The interactive map illustrating geographic distributions, shown in Fig. 1, is created with the Python *folium* library, allowing for the addition of layers and various geographical data to enhance the user experience and provide descriptive information. The maps indicated that the majority of these programs are located in the eastern half of the United States.

The Venn diagram in Fig. 2 illustrates the distribution of the 73 courses across the three themes. It's important to note that a single course can fall under multiple themes simultaneously. Half (51%) of the courses cover security, ethics, and regulations together. Less than one-third (26%) of the courses discuss security and ethics without addressing regulations. Five courses (7%) explore security and regulations together, while approximately 14% focus solely on security and 3% focus solely on regulations in healthcare. There are also dedicated courses that exclusively address ethics in healthcare. Combined with overlapping, there are 71 courses covering security, 56 for ethics, and 44 for regulations in healthcare.

The word cloud analysis for the course descriptions in Fig. 3 reveals that security-related courses emphasize information management, health data security, privacy preservation, and legal and ethical concerns. These courses also cover risks, systems, technology, standards, compliance, and regulations.

NLP analysis on courses in the *Security in Healthcare* theme highlights key areas such as protecting sensitive patient data and maintaining information integrity. Students learn encryption, access control, and data masking techniques. Risk assessment and mitigation strategies are covered, as well as the creation of security policies and procedures, including incident response plans. The courses also discuss the evolving landscape of cybersecurity threats, prevention strategies, authentication methods, network security with firewalls, and secure storage, transmission, and disposal of health information.

The *Ethics* theme courses emphasize ethical principles in healthcare, including patient privacy, informed consent, accountability, transparency, and morality. Students learn about protecting patient confidentiality, ethical use and disclosure of health data, and informed consent practices. These courses promote responsible use of health information and openness in healthcare. Ethical decision-making frameworks help students navigate dilemmas in health information management.

Regulation-themed courses cover the legal and regulatory framework for health professionals. Students learn about laws like HIPAA and HITECH and study regulatory agencies such as the Department of Health and Human Services (HHS) and the Office for Civil Rights (OCR). They discuss industry standards for data security, privacy, and governance to ensure compliance. Students also examine the consequences of non-compliance and enforcement actions taken by regulatory agencies to promote ethical health information management.

TABLE I. The Three Themes and Related Keywords.

Themes	*Keywords*
Security in healthare	security, confidentiality, encryption, risk cybersecurity, authentication, firewall, safety
Ethics in healthare	ethics, consent, privacy, confidentiality, integrity, accountability, transparency, morality
Regulation in healthare	compliance, regulations, HIPAA, legislation, standards, governance, enforcement, policy, law

TABLE II. Program Delivery of the CAHIIM Programs.

Fields	*In-person Only*	*Online Only*	*Both*	*Total*
BS HIM	12	39	22	73
MS HIM	2	11	2	15
MS HI	2	14	12	28

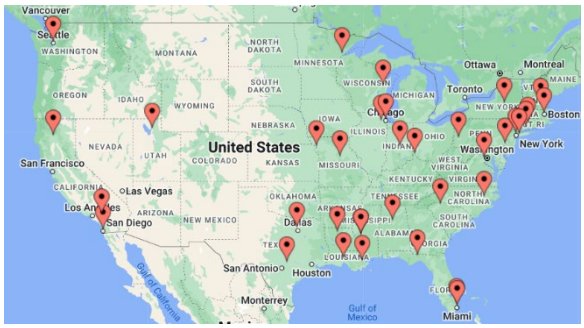

Fig. 1. Geographic location of the CAHIIM accredited programs.

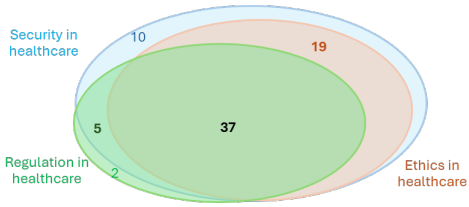

Fig. 2. Geographic location of the CAHIIM accredited programs.

Fig. 3. Word cloud generated based on course descriptions.

IV. Discussions

Findings: The course analysis showed that most cybersecurity training in HIM and HI is primarily didactic and introductory, lacking hands-on components. While these

foundational courses are valuable, there is a clear need to incorporate more experiential learning opportunities to better prepare students for real-world challenges in health data protection and sharing. By offering students practical experience through real-world projects using authentic data and case studies, we can help them develop the skills necessary to effectively address cybersecurity risks in healthcare settings. Developing curricula that emphasize these real-world applications will enhance students' readiness to tackle complex problems and promote best practices in health data protection. Such an approach aligns with the dynamic and evolving nature of cybersecurity in healthcare and ensures that future professionals are well-equipped to safeguard patient information and uphold data integrity.

Limitations: The project is subject to several limitations that may impact the comprehensiveness and accuracy of its findings. First, the analysis focuses exclusively on CAHIIM-accredited programs, which may exclude other relevant programs not covered by CAHIIM accreditation. This limited scope could lead to an incomplete representation of the overall educational landscape in the field. Second, updates from CAHIIM may lag behind program changes, creating discrepancies. For instance, while Temple University's health informatics program is transitioning from MSHIM to MSHI, it is still categorized as MSHIM on the CAHIIM website. Similarly, the University of Pittsburgh's undergraduate program has been revamped to BS in Health Informatics, which is not manifested in CAHIIM program lists. Furthermore, more detailed data collection and analyses are needed to better understand various aspects of cybersecurity training in the health arena, such as their alignment with job market demands and learning outcomes.

V. Conclusions

In conclusion, this study presents an in-depth examination of CAHIIM-accredited programs in cybersecurity training. Out of 116 CAHIIM-accredited programs, only 22 HIM and HI programs from 14 out of 35 institutes offer cybersecurity-related courses. Statistical and geospatial analyses of these programs focus on key themes such as security, ethics, and regulation in healthcare. The analysis of course content identifies the primary areas of emphasis within each thematic category and the overlaps between them. The study also underscores the need for improvement, such as incorporating more hands-on practices, real-world projects using real-world data, and conducting more comprehensive data analysis. Future research and programmatic adjustments should aim to address these gaps and further advance cybersecurity education within HIM and health informatics programs.

Acknowledgment

This work was supported in part by funding from the NSF SaTC EDU award # 2310298.

References

[1] A.A. Adebukola, A. N. Navya, F.J. Jordan, N.J .Jenifer, R.D.Begley. Cyber security as a threat to health care. Journal of Technology and Systems. 2022 Dec 13;4(1):32-64.

[2] A.T. Alanazi . Interprofessional Education in Health Informatics (IPEHI) for Health Sciences Programs. Adv Med Educ Pract. 2023;14:1177-1182. Published 2023 Oct 19. doi:10.2147/AMEP.S422725.

[3] A. C. Norris, & J. M Brittain,. (2000). Education, training and the development of healthcare informatics. Health Informatics Journal, 6(4), 189–195. https://doi.org/10.1177/146045820000600403.

[4] J. S. Patel, O. Oaikhena, TT Phan, H.Vo, J.M. Alizadeh and H. Wu. The Landscape of Health Informatics Education in Low-or Middle-Income Countries. In2023 IEEE 11th International Conference on Healthcare Informatics (ICHI) 2023 Jun 26 (pp. 652-656). IEEE.

[5] Nurul A. Rahman, Intan H. Sairi, Nur A. Zizi, Fadhilah Khalid. The importance of cybersecurity education in school. International Journal of Information and Education Technology. 2020 May;10(5):378-82.

[6] W. Newhouse, S. Keith, B. Scribner, G. Witte. National initiative for cybersecurity education (NICE) cybersecurity workforce framework. NIST Special Publication. 2017 Aug;800(2017):181.

[7] A.A. Adebukola, A.N. Navya, F.J. Jordan, N.J. Jenifer, R.D. Begley. Cyber security as a threat to health care. Journal of Technology and Systems. 2022 Dec 13;4(1):32-64.

[8] D. Branley-Bell, L. Coventry, E. Sillence. Promoting cybersecurity culture change in healthcare. In Proceedings of the 14th Pervasive Technologies Related to Assistive Environments Conference, 2021 Jun 29; pp. 544-549.

[9] N. O'Brien, S. Ghafur, M. Durkin. Cybersecurity in health is an urgent patient safety concern: we can learn from existing patient safety improvement strategies to address it. Journal of Patient Safety and Risk Management. 2021 Feb;26(1):5-10.

[10] M. Waddell. Human factors in cybersecurity: Designing an effective cybersecurity education program for healthcare staff. In Healthcare Management Forum, 2024 Jan; Vol. 37, No. 1, pp. 13-16. Sage CA: Los Angeles, CA: SAGE Publications .

[11] M.J. Swede, V. Scovetta, M. Eugene-Colin. Protecting patient data is the new scope of practice: A recommended cybersecurity curricula for healthcare students to prepare for this challenge. Journal of Allied Health. 2019 Jun 6;48(2):148-56.

[12] J. Qiu, L. Li, J. Sun, J. Peng, P. Shi, R. Zhang, B. Lo. Large AI models in health informatics: Applications, challenges, and the future. IEEE Journal of Biomedical and Health Informatics. 2023.

[13] J. S. Patel, B. Dzomba and H. Wu "Think Outside of Box"-Ten Commandments in Providing Optimal Health Informatics Education. In2022 IEEE 10th International Conference on Healthcare Informatics (ICHI) 2022 Jun 11 (pp. 585-590). IEEE.

[14] W.J. Gordon, A. Wright, R.J. Glynn, J. Kadakia, C. Mazzone, E. Leinbach, A. Landman. Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. Journal of the American Medical Informatics Association. 2019 Jun;26(6):547-52.

[15] F. Rizzoni, S. Magalini, A. Casaroli, P. Mari, M. Dixon, L. Coventry. Phishing simulation exercise in a large hospital: A case study. Digital Health. 2022 Mar;8:20552076221081716.

[16] R.S. Cheung, J.P. Cohen, H.Z. Lo, F. Elia. Challenge based learning in cybersecurity education. In Proceedings of the International Conference on Security and Management (SAM), 2011; p. 1. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

[17] G. Jin, M. Tu, T.H. Kim, J. Heffron, J. White. Evaluation of game-based learning in cybersecurity education for high school students. Journal of Education and Learning (EduLearn). 2018 Feb 1;12(1):150-8.

[18] M.D. Workman, J.A. Luevanos, B. Mai. A study of cybersecurity education using a present-test-practice-assess model. IEEE Transactions on Education. 2021 Jun 11;65(1):40-5.

[19] M. Waddell. Human factors in cybersecurity: Designing an effective cybersecurity education program for healthcare staff. In Healthcare Management Forum, 2024 Jan; Vol. 37, No. 1, pp. 13-16. Sage CA: Los Angeles, CA: SAGE Publications.

[20] M.J. Swede, V. Scovetta, M. Eugene-Colin. Protecting patient data is the new scope of practice: A recommended cybersecurity curricula for healthcare students to prepare for this challenge. Journal of Allied Health. 2019 Jun 6;48(2):148-56.

[21] Commission on Accreditation for Health Informatics and Information Management Education, https://www.cahiim.org/. [Last accessed: 04/21/2024].