The University Senate of Michigan Technological University

Proposal 47-20

Establishment of a New Graduate Certificate in Security and Privacy in Healthcare

Submitted by:
Master of Science in Health Informatics (MSHI) Program
Department of Applied Computing
College of Computing

1. **Proposal Date:** March 2, 2020

2. **Proposing Contacts and Departments:** Guy Hembroff, Health Informatics Graduate Program Director, hembroff@mtu.edu

3. **Sponsor Department Approvals:** NA

4. **General Description and Characteristics of Certificate**

   The department of Applied Computing's Health Informatics graduate program within the College of Computing at Michigan Tech proposes a nine credit Certificate named Security and Privacy in Healthcare. Careers in this area protect the security and privacy of healthcare information. Hospitals, clinics, private practices, security firms, corporations, government units, and insurance companies hire individuals with skills associated with the Security and Privacy in Healthcare Certificate.

   The proposed certificate provides individuals with the ability to secure and protect the privacy of health information, comply with state and federal healthcare data regulations, ensure interoperability in the exchange of healthcare data, and ensure healthcare systems are capable of successfully adopting new technologies to improve the quality and efficiency of patient care.

5. **Rationale for the Certificate**

   The healthcare industry relies on digital health, technology, and its connection to the Internet. Disrupted systems, intentionally or accidentally, can jeopardize patient safety, privacy, and health outcomes, leading to the rising cost of healthcare expenditures. Protecting patient data, stored or in transit, is critical. Healthcare security professionals can use their knowledge of medical standards, compliance, and interoperability with their understanding of security and privacy concepts, methods, and tools to:

   - Identify applicable regulations, compliance frameworks, privacy principles and policies to protect information security;
   - Understand the disparate nature of sensitive data and handling implications;
   - Acquire, preserve, investigate, and recover data and digital devices; and

- Lead or participate in the development and implementation of safeguards to protect sensitive information.

The Certificate documents an individual's completion in the specialization of security and privacy in the healthcare field for current/future employers. Additionally, the Security and Privacy in Healthcare Certificate is stackable with the proposed Artificial Intelligence in Healthcare Certificate. This provides students with an opportunity to acquire two specializations in critical and expanding areas of computing and healthcare, while working towards a MS in Health Informatics.

6. Related Programs

- Boston University (https://www.bu.edu/met/programs/graduate/medical-information-security-privacy-certificate/)
- Capella University (https://www.capella.edu/online-degrees/certificate-information-assurance-cybersecurity/)
- Indiana University and Purdue University (https://soic.iupui.edu/biohealth/graduate/health-informatics/health-information-security/)

7. Projected Enrollments

It is projected that enrollment in the certificate program will primarily consist of: a) on campus students from Michigan Tech who are enrolled in the Health Informatics, Cybersecurity, or Data Science graduate programs and have taken one or more of the shared courses between curriculums (e.g. SAT 5111, SAT 5816, SAT 5817); and b) online students currently working within a clinical or information technology environment and wish to gain continuing education in the areas of security and privacy in healthcare to help further their careers.

Table 1: Security and Privacy in Healthcare Certificate Projected Enrollment

Academic Semester	On Campus Projected Enrollment	Online Projected Enrollment	Total Enrollment
Fall 2020	5 students	2 students	7 students
Fall 2021	7 students	3 students	10 students
Fall 2022	8 students	4 students	12 students
Fall 2023	10 students	6 students	16 students
Fall 2024	12 students	8 students	20 students

8. Scheduling Plans

The coursework will be offered during regular instructional time periods and will not require changes to scheduling of classes.

9. Curriculum Design

Required Coursework – 6 credits

- SAT 5111: Security and Privacy (3 credits) – offered in the fall
- SAT 5817: Security Penetration Test and Audit (3 credits) – offered in the spring

Elective Coursework – 3 credits

- SAT 5241: Designing Security Systems (3 credits) – offered in the spring
- SAT 5283: Information Governance and Risk Management (3 credits) – offered in the fall
- SAT 5816: Digital Forensics (3 credits) – offered in the fall

Students pursuing the Certificate of Security and Privacy in Healthcare will work with their advisors to choose the best elective course, given area of interest and prior coursework.

10. Course Descriptions

- SAT 5111- Security and Privacy (3 credits): Examines key health information security, policy, and procedures. Investigates how to distinguish elements of a security audit and key security policies. Analyzes the roles of people maintaining health information security and explains elements of these roles within the organization. Semester offered: Fall. Prerequisite: none
- SAT 5817 - Security Penetration Test and Audit (3 credits) : Provides knowledge and demonstrated methods to help prevent security breaches and develop safeguards to protect sensitive information and confidential data. Primary focus will be on the healthcare sector. Students learn offensive and defensive security concepts, audit best-practices. Semester offered: Spring. Prerequisite: none
- SAT 5241 - Designing Security Systems (3 credits): Provides an overview of techniques used in the design of secure systems with a primary focus on real-world case studies. Students will examine attacks on deployed systems and investigate how these vulnerabilities have been addressed. Practical advantages and shortcomings of several notions of provable security will also be examined. Students will be expected to read, understand, and present recent research papers. Semester offered: Spring. Prerequisite: SAT 5111
- SAT 5283 - Information Governance and Risk Management (3 credits): Examines the legal and regulatory requirements and security privacy concept principles regarding healthcare information. Best practices of how organizations manage information risk through risk assessment practices and procedures will be conducted. Semester offered: Fall. Prerequisite: none
- SAT 5816 - Digital Forensics (3 credits): Introduction of the basic principles and technology of digital forensics, including acquisition, preservation, and recovery and investigation of the evidence stored in digital devices. Semester offered: Fall. Co-requisite: SAT 5111

11. Model Schedule Demonstrating Completion Time

The Certificate is designed to be completed over a two-semester sequence.

Fall Semester	**Spring Semester**
SAT 5111: Security and Privacy	SAT 5817: Security Penetration Test and Audit

Students will complete the Certificate requirements through taking an elective course in either Fall (SAT 5283 or SAT 5816) or Spring (SAT 5241) semester.

The Certificate can be completed on-campus or online, as the MSHI has established its full curriculum online. All MSHI faculty are certified for online instruction.

12. Library and other Learning Resources

No new library or other learning resources will be required by the MSHI program

13. Faculty Resumes

- Dr. Yu Cai, PhD, Professor
- Dr. Guy Hembroff, PhD, Associate Professor
- Dr. Donald Peck, PhD, Professor of Practice
- Dr. Jinshan Tang, PhD, Professor
- Dr. Weihua Zhou, PhD, Assistant Professor

All Faculty Curriculum Vitae can be found at: https://www.mtu.edu/health-informatics/people-groups/faculty/

14. Equipment

No additional equipment will be required.

15. Program Costs

No additional costs are anticipated. Current faculty resources would support enrollment growth of 35 students for the Artificial Intelligence in Healthcare Certificate and 40 students for the Security and Privacy in Healthcare Certificate, totaling 75 students (at a 15:1 ratio) for the two stackable certificates. Charges for any software not provided through gratuitous educational licenses can be recovered through appropriate course lab fees.

16. Space

No additional space will be required.

17. Policies, Regulations, and Rules

Not Applicable

18. Accreditation Requirements

Adding this certificate program will not result in any change to accreditation requirements. The Security and Privacy in Healthcare Certificate will automatically become subject to periodic review with the Health Informatics graduate program.

19. Planned Implementation Date

Fall 2020

20. Assessment

An overview of the Health Informatics Graduate Learning Objectives used for the assessment of the Security and Privacy in Healthcare Certificate are as follows:

- GL01 - Demonstrate proficiency of the subject matter.

- GL02 - Demonstrate knowledge of core competencies in selected, complementing areas of the subject matter.
- GL05 - Demonstrate professional skills (oral, written, and practice of responsible conduct of the profession).

Table 2: Health Informatics Graduate Learning Objectives for Certificate Assessment

Assessment Points	**Graduate Learning Objectives (GLO)**
Grades in certificate courses (SAT 5111, SAT 5817, SAT 5841, SAT 5283, SAT 5816)	GLO1, GLO2
Course Instructor is Responsible for completing Class Communication Evaluation	GL05