# Developing the CARES Framework to Secure IoT Devices in Small-Practice Healthcare Facilities with MAXIMUS

A Professional Readiness Experiential Program (PREP) Project Effort

----- ***Authors / Student Project Team Members*** -----

**Zach Gentry** is a student at George Mason University graduating with a bachelor's degree in Management Information Systems and Business Analytics. Passionate about leveraging data-driven insights to solve complex problems, he aims to contribute to innovative solutions in business analytics and technology-driven environments after graduation.

**Fawzia Hamdard** is a student at George Mason University graduating with a bachelor's degree in Management Information Systems. She is currently working as a Member Advisor at Apple Federal Credit Union. She plans to contribute to the financial industry by developing innovative technology and cybersecurity solutions. Her goal is to enhance the security and efficiency of financial services through creative approaches.

**Melinda Nguyen** is a student at George Mason University graduating with a bachelor's degree in Management Information Systems. She works as an administrative assistant for Conceras, an IT Consulting company located in McLean, Virginia. She is interested in one day transferring her knowledge in technology and analytics to work in the energy sector.

----- ***Industry Participant / Mentor*** -----

**Kynan Carver**
Cybersecurity Managing Director
MAXIMUS

----- ***Faculty Member*** -----

**Brian K. Ngac, PhD**
Instructional Faculty & Dean's Teaching Fellow
George Mason University's Costello College of Business
bngac@gmu.edu

***Interested in being an Industry Participant and or PREP Sponsor? Please reach out to bngac@gmu.edu, Thanks!***

**--- Client Testimonial ----**

*"The research conducted examined the implications of HIPAA on small hospital systems and explored strategies for achieving compliance. The C.A.R.E.S. system is unlikely to diminish the overall effort required from healthcare providers, as HIPAA mandates that all healthcare organizations fully comply with its regulations. The analysis provided significant insights into IoT security, along with high-level recommendations for remediation and best practices.*

*These recommendations align with established industry standards and are presented in a structured format that facilitates the organization of IT systems for providers. Comprehending HIPAA can prove particularly challenging for small practices that do not possess dedicated IT or security teams. By delineating compliance into specific areas, smaller organizations can concentrate on the most critical elements of security that may be overlooked by personnel without IT expertise. This solution offers a comprehensive overview of best practices and security implementations, accompanied by a retrospective analysis of how these measures might have mitigated past incidents."*

*- Kynan Carver | Cybersecurity Managing Director | MAXIMUS*

## Introduction

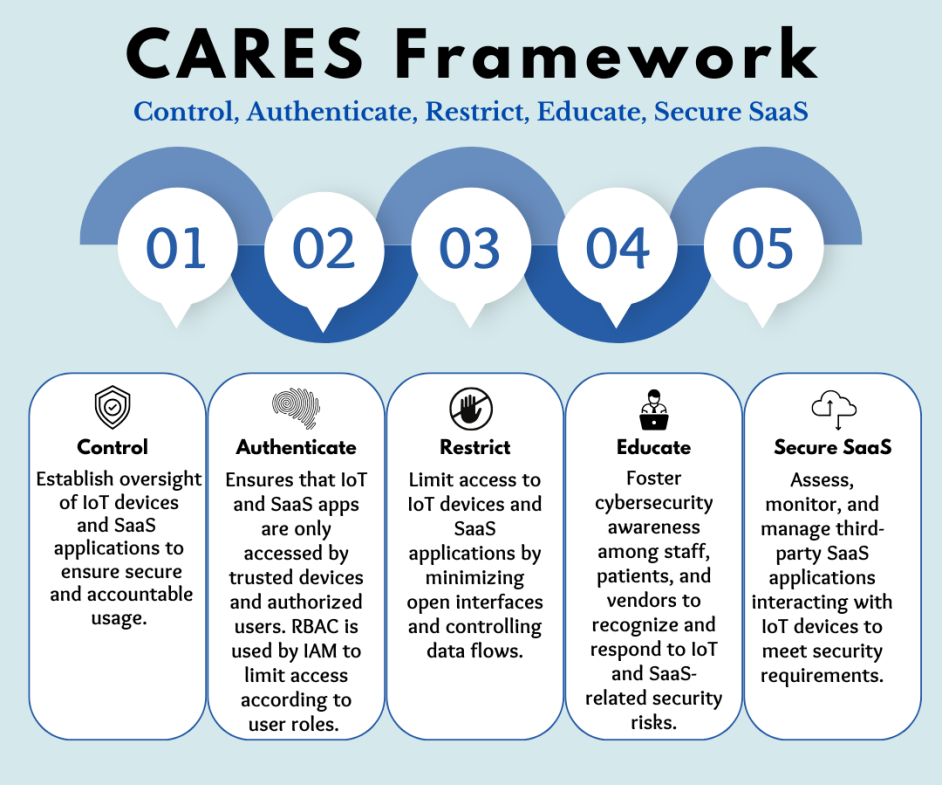
During the Fall 2024 semester, GMU PREP students Zach Gentry, Fawzia Hamdard, and Melinda Nguyen partnered with Maximus to research the rapidly growing Internet of Things (IoT) and propose novel security solutions to address vulnerabilities pervasive in the field of healthcare.

## Business Challenge

Initially presented with the broad research topic of IoT, the students collaborated with Maximus over the course of ten weeks to narrow down the business challenge: ***securing IoT devices in small-practice healthcare facilities***. The healthcare industry is a particular point of interest for the unique conditions that it presents: a lack of adequate security controls for IoT devices and systems in healthcare facilities despite widespread and intensive use (which heightens patient risk), industry-specific resource constraints, and industry-prevalent change resistance. Due to the restricted nature of cybersecurity in healthcare, attributed to limited financial resources and access to professional cybersecurity expertise, the goal of the project was to develop a clear and accessible security solution. Additionally, to manage expected change resistance, a robust change-management process must be integral to the proposed solution.

## Activities Done to Address the Business Challenge

Through weekly meetings with Maximus, the PREP student team gathered the necessary requirements, resources, and additional guidance to tackle the project. The students produced a paper detailing the current cybersecurity environment in the healthcare sector which introduced the Control, Authenticate, Restrict, Educate, Secure SaaS (CARES) Framework to enhance IoT security.



The application of the CARES framework was demonstrated through a use case, where it was applied to the 2019 Wood Ranch Medical ransomware attack. The attack permanently encrypted all patient records and made data irrecoverable; the facility was unable to recover and consequently shut down. The use case details how each pillar of the CARES framework could have been applied in this case – and the damage that it would have mitigated. For example: Wood Ranch Medical should have taken steps to ensure they worked with the secure SaaS vendors, who would've provided secure, cloud system backup – a precaution that would have prevented the devastating data loss.

**Results & The Positive Impact**

The CARES Framework and the overall paper that introduced it were well-received by Maximus following a presentation delivered by the PREP students. A point of discussion included future steps and project implementation plans. The PREP student team is looking to submit their article for publication in a cybersecurity journal (i.e., ISACA Journal). Meanwhile, Maximus has their own plans for the deliverable. Maximus Cybersecurity Lead Kynan Carver will be referencing the paper at a healthcare conference early 2025. Besides this, future Maximus-sponsored researchers and/or students will further develop the research produced, including conducting a cost-benefits analysis of the CARES Framework and collecting relevant industry data to make more recommendations at the technical level. Additionally, as a service provider to a wide network of healthcare entities, including Medicare and Medicaid, Maximus will be able to apply the CARES Framework in a meaningful manner.

Overall, the work done throughout this project has shone a necessary spotlight on small-practice healthcare entities, the challenges they face with IoT security, and a guiding framework to help them mitigate those cybersecurity challenges.

**Conclusion**

Though the project requires additional research and development, Zach, Fawzia, and Melinda have laid the foundation necessary for advancing healthcare IoT cybersecurity for small-practice healthcare entities. The need for security solutions in this sector only grows more urgent by the day – and now is the time to address it.

**PREP Student Reflection**

As we finalize our project, we reflect positively on our time in PREP and the hours we spent working alongside the Maximus representatives. The program provided us with invaluable work experience and advice from industry professionals from Maximus, offering a hands-on learning opportunity that simply can't be replicated in the classroom. The prompt also allowed us to expand our critical-thinking and problem-solving skills, pushing us to consider certain cybersecurity topics we had never explored before. Finally, the project gave us the chance to explore our post-graduation career interests and introduced us to an exciting and novel cybersecurity sector—an experience that we believe will open opportunities for us in the future.