****

**UC Tech Awards 2023 Form**

 **Category:** IT SECURITY
**Name:** The Risk and Safety Solutions HIPAA Project (4)
**Number of people:** (4)
**Location:** UC Office of the President

1. **Person submitting the application/nomination**
	1. Emily Slonim, Lead Communications Analyst, Risk and Safety Solutions, UCOP, Staff
	2. **Email address:** eslonim@ucdavis.edu
	3. **The name of your organization:** Risk and Safety Solutions
2. **Award category** IT Security Award
3. **Name of person, name of the team, or name of the project to receive the award**
4. **All project team members - if applicable**

Trevin Haseltine tjhaseltine@ucdavis.edu

Project Management Coordinator, Risk and Safety Solutions, Staff

Stefan Tomic sttomic@ucdavis.edu

Information Security Officer, Risk and Safety Solutions, Staff

Dinesh Buddha, dbuddha@ucdavis.edu

Security Administrator, Risk and Safety Solutions, Staff

Jesus Cipriano-Vasquez jcvasq@ucdavis.edu

Security Administrator, Risk and Safety Solutions, Staff

1. **Which location was affected by the work?** All UC campuses and Health Centers
2. **Summary**

The RSS Security Team at Risk and Safety Solutions (RSS) has been nominated for the IT Security Award at the UC Tech Awards 2023 for their work in achieving HIPAA compliance to protect sensitive patient health information at University of California (UC) Health Centers. The team's project involved an evaluation of RSS security protocols and federal requirements, as well as improvements to administrative, physical, and technical safeguards, policies, procedures, and documentation.

1. **Narrative**

Risk and Safety Solutions (RSS) serves the ten UC campuses and five medical centers with safety solutions, and in 2020, the RSS security team identified a need to be HIPAA compliant. HIPAA, or the Health Insurance Portability and Accountability Act, is a federal law that sets national standards to protect sensitive patient health information from being disclosed without the patient’s consent or knowledge. As RSS expanded in the healthcare field, so did the imperativeness of protecting the sensitive data of UC Health Centers and the individuals they serve.

The RSS Security team began the HIPAA project with an evaluation of RSS security protocols and a review of the federal requirements. HIPAA compliance is measured using the HIPAA Privacy Rule, the HIPAA Security Rule, and the HIPAA Breach Notification Rule. For RSS, the evaluation is based on the Security Rule and the Breach Notification Rule, as the Privacy Rules do not apply. RSS also has to consider the electronically protected health information (ePHI) environment where the data is stored. The initial steps in the project were intended to identify potential shortcomings and assess the feasibility of the endeavor. There were twenty-three standards that had to be met in the categories of administrative, physical, and technical safeguards; organizational requirements; and policies, procedures, and documentation requirements.

The team created an estimated project kickoff timeline from April to June 2020 and worked closely with stakeholders to determine the necessary resources. The plan included 1) risk analysis, 2) vulnerability management, 3) identity access management, 4) system inventory and data management, 5) system architecture, 6) application architecture, 7) logging and monitoring inventory systems, 8) evaluate high compliance, 9) change management, 10) business continuity plan, 11) disaster recovery plan, 12) incident response, 13) staff policies and procedures, 14) physical security, and finally 15) business associate agreements and vendor contracts.

Out of the twenty-three standards outlined by the HIPAA Security Rule, the RSS Security team identified key areas of improvement within the RSS security system. For administrative safeguards, existing policies had to be revised and new policies had to be created to meet HIPAA requirements. The RSS Security team was able to leverage existing reporting capabilities to create a monthly report that would list all unusual access. Policy adjustments were also made with technical and physical safeguards to include contingency operations in case of a breach.

The RSS Security team enlisted the help of a third-party vendor, Cynergistek, to complete a risk analysis and evaluate RSS for HIPAA compliance. Cynergistek conducted an analysis of RSS’ security measures in May of 2020, and the analysis included an Information Security Program Assessment (ISPA) using the Cybersecurity Framework (CSF) published by the National Institute of Standards and Technology (NIST).

The assessment focused on whether RSS met the needs of the healthcare industry, specifically the HIPAA Security Rule and the HIPAA Breach Notification Rule. It was determined that overall, RSS scored 80%, which was 12% above the industry average. Based on the data provided, RSS met the minimum requirements to be considered HIPAA compliant. However, the Security team reviewed the recommendations made by Cynergistek and determined that changes could be made to improve the score further.

In 2021, Cynergistic completed another risk analysis to evaluate RSS for HIPAA compliance, and thanks to the diligent work of the security team, RSS received a 96%, which at the time was 34% higher than the industry average. In 2022, another third-party vendor, Coalfire, with more stringent assessment parameters, evaluated RSS HIPAA compliance, and again, RSS outperformed the industry standard in every category.

Over the past three years, the RSS Security team has taken an iterative approach to meeting and exceeding HIPAA compliance requirements. Feedback from the most recent assessment is currently being implemented, and the team is hopeful that the 2023 assessment will continue to show improvements toward HIPAA compliance measures. The problem the RSS Security team faced was complex, as it required an overhaul of the security policies and practices in use. It involved scrutinizing current practices and out-of-the-box thinking to address the industry needs, and as the data shows, the RSS Security team rose to the challenge and surpassed their goal. The exact number of individuals impacted by the RSS Security Team HIPAA project is nearly incalculable, as it affects every patient in the University of California Medical System, however, as of 2021, the UC Medical System serves approximately 4 million patients annually.

I am nominating the RSS Security team’s HIPAA project for the UC IT Security Award because of their dedication to protecting the private health information of millions of people by leveraging technology to implement safeguards. By striving for excellence in data security, the RSS Security team demonstrated integrity, innovation, and accountability to complete the project.