**Item 6**

**Project Proposal**

Submitted to: Dr. Ferrell

Submitted by: Shirdora Ashe

February 23, 2024

**Abstract**

**In modern healthcare systems, the secure and efficient sharing of patient data among healthcare providers is a challenge. There is a pressing need for a solution to safeguard patient privacy, enhance care coordination, and ensure compliance with HIPAA. An open-source software solution could provide a secure, efficient, and user-friendly way to share patient data. Some strengths of this solution are that utilizing open-source software components, reducing licensing costs, promoting community-driven development and support, and flexible deployment options, cater to diverse organizational needs and preferences. Some weaknesses that this solution has are that there needs to be more centralized support and accountable mechanisms may pose challenges in troubleshooting and resolving technical issues. The proposed solution is a better solution than the alternative. The proposed solution prioritizes security and compliance from the ground up, offering comprehensive data protection measures out-of-box. The user-friendly interface and seamless integration capabilities streamline adoption and usage, minimizing training requirements and maximizing efficiency.**

# Problem Background

In the increasingly digitized landscape of modern healthcare systems, the critical need for secure and efficient data sharing among healthcare providers has emerged as a pressing challenge, necessitating innovative solutions to safeguard patient privacy, enhance care coordination, and ensure compliance with stringent regulatory standards such as HIPAA. This problem has caused major problems for the healthcare system as the lack of security leads to delays in care for patients. For example, in 2016, MedStar Health delivery systems were attacked with ransomware being down for 48 hours. Three of the main systems- inpatient health records, outpatient records, and the registration and scheduling system- were brought offline by the attack. (*Medstart: No ransom paid in cyber attack, 2023* ) The number of attacks has increased drastically affecting millions of patients. In a study conducted by students from the universities of Minnesota, and Florida, between 2016 and 2021, there were “documented 374 ransomware attacks on” a healthcare facility that “affected the Patient Health Information of nearly 42 million patients.” (Neprash, et al, 2020 ) The healthcare system has “a large number of weak points due to third-party lenders, patient data practices, connected medical devices, supply chain issues, and outdated systems or software.” (*Kancherla*,  *2023*) The need for updating systems and more secure practices and software is great. This problem needs a more efficient and secure sharing application or system to prevent unauthorized access from third parties.

# Literature/Technology/Professional Environment Review

Currently how the healthcare system uses different methods to share data between providers is leaving it open to attacks. Data sharing is “the exchange of information between individuals, departments, organizations, and systems to facilitate collaboration, decision making, and analysis. (*Devane, 2023* ) Securing data, especially, in healthcare is important because the data being held is sensitive to patient privacy. Data breaches and the holding of data from ransomware attacks can have deadly consequences. The systems that hold data need to follow some simple best practices. One of the practices would be building data security measures into the tech stacks. When creating the tech stack for the healthcare application make sure that security measures are added to the foundation. The traditional approaches used for security, “like perimeter defenses and static access controls” will not work for data protection. (*Devane, 2023)*

# Project/Problem Justification

In modern healthcare systems, the secure and efficient sharing of patient data among healthcare providers remains a significant challenge. Existing methods often lack robust security measures and may not be optimized for efficiency hindering timely and effective patient care. ( *Hulsen, 2020*)There is a pressing need for a comprehensive solution that facilitates seamless and secure data sharing among healthcare providers while prioritizing patient privacy and regulatory compliance. The primary target of this project is healthcare workers, including physicians, nurses, and administration staff, who require timely access to accurate patient information for treatment. Additionally, patients are beneficiaries of this project as they benefit from improved coordination of care and enhanced privacy protection. The significance of this project lies in its potential to improve healthcare delivery by providing a secure, efficient, and user-friendly platform for sharing patient data.

# Assumptions

An assumption that can be made about the capabilities of the project manager is that the manager possesses technical skills in software development in software development. The manager has adequate knowledge of data security. They also have access to material about the problem and solutions.

# Constraints

A constraint of the project manager may need more time, expertise, and experience.

Barriers to the completion of the project:

* Technical Challenges: Software bugs, compatibility issues, and integration complexities may arise during the development process.
* Regulatory hurdles related to compliance with healthcare data privacy laws (eg. HIPAA) may be necessary to manage with careful planning.
* Limited access to real-world healthcare data for testing and validation may pose challenges in ensuring the platform’s efficacy and accuracy.

Anticipated barriers to Large-Scale Implementation:

* Resistance to change within healthcare organizations may impede the adoption of new data-sharing technologies
* Concerns about data security, privacy, and liability may need to be addressed to gain stakeholder’s trust and support
* Integration with existing healthcare IT systems and workflows may require significant time and effort

# Analyze Multiple Solutions

The proposed solution has some strengths and weaknesses. One of those strengths is the user-friendly interface and navigation improves usability, which could result in higher adoption rates among healthcare professionals. This solution hopes to have robust security measures ensuring the confidentially and integrity of patient data, complying with healthcare data privacy regulations. The weaknesses that may follow this solution are: the initial development and implementation costs may be relatively high due to the need for robust security infrastructure and compliance measures; ongoing maintenance and support requirements may necessitate additional resources and expertise; and dependency on external factors such as internet connectivity and system reliability may introduce operational risks and downtime. An alternative solution is to use open-source software to create a new application for sharing data. Some strengths of this solution are that utilizing open-source software components, reducing licensing costs, promoting community-driven development and support, and flexible deployment options, cater to diverse organizational needs and preferences. Some weaknesses that this solution has are that there is a lack of centralized support and accountable mechanisms may pose challenges in troubleshooting and resolving technical issues. The proposed solution is a better solution than the alternative. The proposed solution prioritizes security and compliance from the ground up, offering comprehensive data protection measures out-of-box. The user-friendly interface and seamless integration capabilities streamline adoption and usage, minimizing training requirements and maximizing efficiency.

# McCumber's Cube

When it comes to McCumber’s Cube dimension of confidentiality, the secure and efficient data-sharing platform prioritizes confidentiality by implementing robust security measures. Confidentiality according to the McCumber Cube is “ the assurance that information is not disclosed to unauthorized persons, processes or devices. The application of this security service implies information labeling and need-to-know imperatives are aspects of the system security policy” (*Maconachy,2001*) Through strong encryption techniques and access control systems, the platform ensures that sensitive patient information remains confidential. Integrity according to the McCumber Cube, “is the quality of an information system reflecting logical correctness and reliability of an operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data.” (*Maconachy,2001*) Ensuring the integrity of patient data is paramount in healthcare systems, as any unauthorized modification or tampering could have serious implications for patient care. The proposed solution incorporates measures to safeguard data integrity, such as audit trails and secure communication protocols. In the context of healthcare, the availability of patient data is crucial for providing timely and effective care. The proposed solution is designed to maximize data availability by ensuring continuous access to patient records for authorized healthcare providers. Measures to ensure continuous availability are redundancy measures and disaster recovery plans to minimize downtime and ensure uninterrupted access to crucial healthcare information.

# Project Proposal

The proposed project is a new secure and efficient data-sharing application for healthcare providers. The methodology of this project will include, requirement gathering and analysis to understand user needs and systems specifications. The project manager has access to someone who works in the healthcare system who can gather these requirements. The design and prototyping of the platform’s architecture, user interface, and security features. Implementation and testing of core functionalities, including authentication, encryption, and data retrieval.

# Conclusion

In conclusion, the Secure and Efficient Data sharing application represents a holistic solution to the challenges of healthcare data sharing, addressing the critical dimensions of confidentiality, integrity, and availability as outlined by the McCumber Cube framework. By providing robust security measures, user-friendly interfaces, and scalability, the application not only safeguards patient privacy and data integrity but also ensures continuous access to critical healthcare information for timely patient care. With its comprehensive approach to information security, the application has the potential to revolutionize healthcare delivery by facilitating seamless data sharing among providers while mitigating the risks posed by cyber threats.

# References

Devane, H. (2023, July 28). *5 Best Practices for Secure Data Sharing*. Immuta. https://www.immuta.com/blog/secure-data-sharing/

Fabian, B., Li, M., Hevner, A., & Peffers, K. (2014, May 29). *Collaborative and secure sharing of healthcare data in multi-clouds*. Information Systems. https://www.sciencedirect.com/science/article/abs/pii/S030643791400088X

Hulsen, T. (2020, May 17). *Sharing Is Caring—Data Sharing Initiatives in Healthcare*. National Library of Medicine. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7246891/

Kancherla, S. (2023, August 14). *Ransomware in Healthcare: Understanding the challenges - vmware ...* VMware . <https://blogs.vmware.com/industry-solutions/2023/08/14/ransomware-in-healthcare-understanding-the-challenges/>

Maconachy, V., Schou, C., Ragsdale, D., & Welch, D. (2001, June 5). McCumber Cube 2001. West Point; IEEE Workshop in Information Assurance and Security.

*MedStar: No ransom paid in cyber attack: WBAL Baltimore News*. WBAL News Radio. (2023, July 7). https://www.wbal.com/medstar-no-ransom-paid-in-cyber-attack/

Neprash, H., McGlave, C., Cross, D., Virnig, B., Puskarich, M., Huling, J., Rozenshtein, A., & Nikpay, S. (2022, December 29). *Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021*. National Library of Medicine. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9856685/#:~:text=In%20this%20cohort%20study%20conducted,of%20nearly%2042%20million%20patients

Virkkula, J. (2023, September 14). *5 secure data sharing challenges in healthcare*. SSH. https://www.ssh.com/blog/5-secure-data-sharing-challenges-in-healthcare#:~:text=When%20medical%20data%20is,hacked%2C%20stolen%2C%20and%20misused

ZhangT., ZhangC., SinghS., YuehongY., FirouziF., LiuY., DasS., LiuH., WangK., SunJ., ZhangB., YangW., LiuJ., MasudM., GhoumidK., GayathriN., & ShamirA. (2023, July 29). *Enabling efficient and secure health data sharing for healthcare IOT Systems*. Future Generation Computer Systems. https://www.sciencedirect.com/science/article/abs/pii/S0167739X23002881