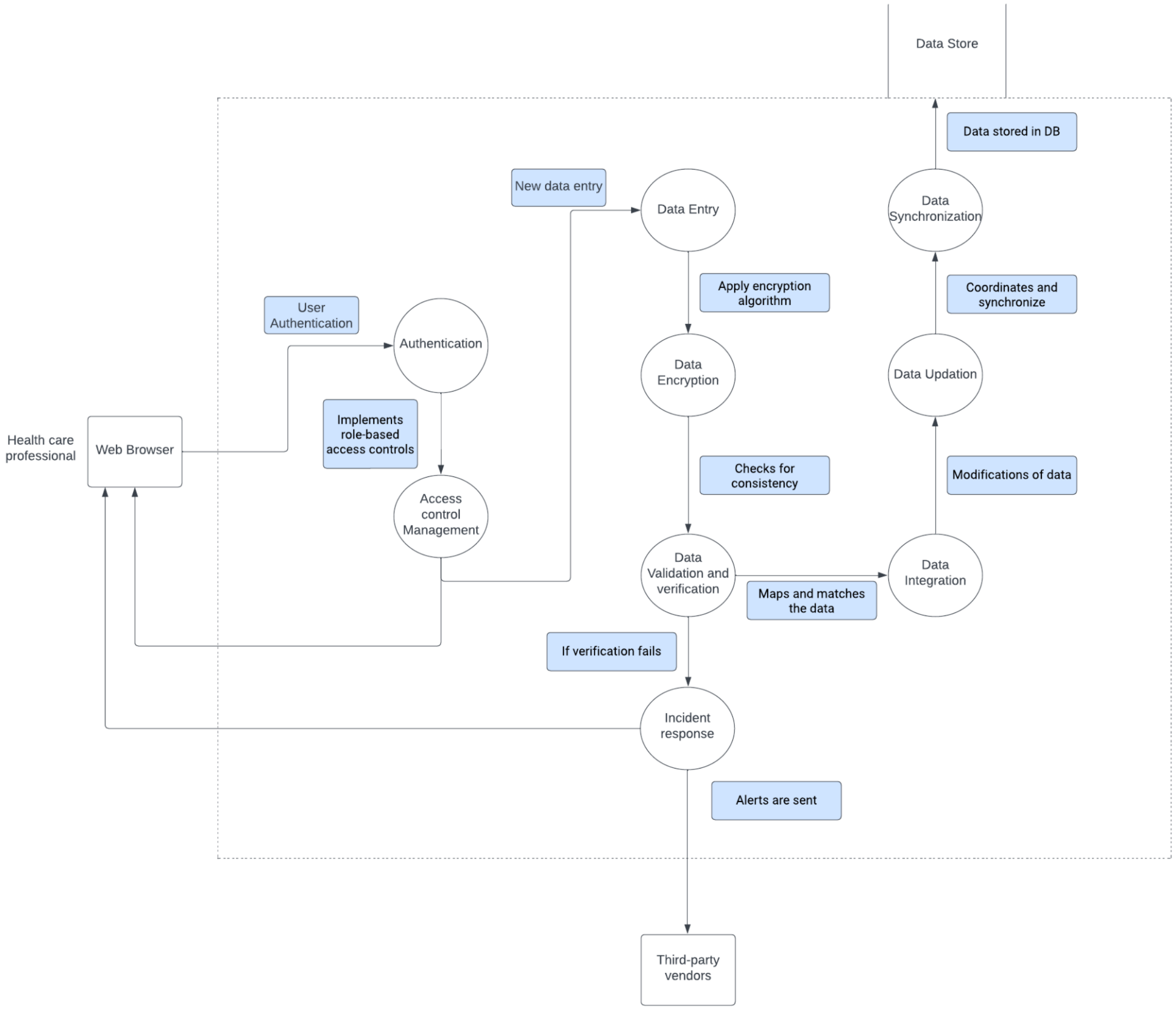
CHAPTER 1: INTRODUCTION

Abstract:\\

This case study focuses on the implementation of robust cybersecurity measures within an Electronic Health Records (EHR) system. EHR systems play a crucial role in modern healthcare, storing sensitive patient information and facilitating efficient data sharing among healthcare providers. However, their widespread adoption has also made them attractive targets for cyberattacks. This case study examines the cybersecurity challenges faced by a healthcare organization and explores the measures taken to protect their EHR system from potential threats.\\



DFD - Green Health

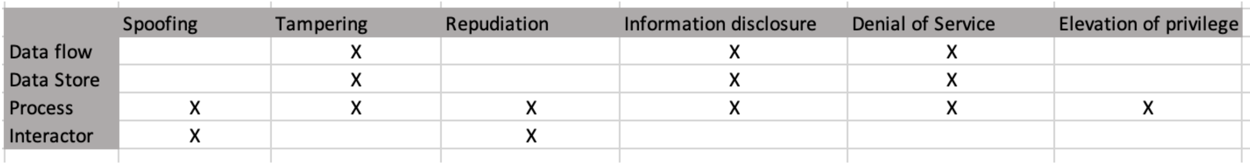
CHAPTER 2: THREAT ANALYSIS

I chose STRIDE method for threat analysis for the system.\\

By applying the **STRIDE** method, organizations can identify specific threats that could impact the security and integrity of their EHR system. This enables them to implement targeted security measures to mitigate the identified threats effectively and protect the confidentiality, integrity, and availability of patient data within the EHR system.\\

Below points address threats in an Electronic Health Records (EHR) system when STRIDE method is applied.\\

1.Spoofing:Strong user authentication mechanisms, such as multi-factor authentication, to ensure that only authorized users can access the system.\\
2.Tampering:Implement data integrity controls, such as cryptographic hashing, to ensure the integrity of stored data and detect any unauthorized modifications.\\
3.Repudiation: Implement robust audit logging mechanisms to record and store detailed information about user actions and system activities.\\
4.Information Disclosure:Employ strong access controls to ensure that only authorized users can access sensitive information.\\
5.Denial of Service:Implement network traffic filtering, firewalls, and intrusion prevention systems to detect and block malicious traffic or DoS attacks.\\
6.Elevation of Privilege:Implement the principle of least privilege, granting users only the necessary access and permissions required to perform their tasks.\\



	Spoofing	Tampering	Repudiation	Information disclosure	Denial of Service	Elevation of privilege
Data flow		X		X	X	
Data Store		X		X	X	
Process	X	X	X	X	X	X
Interactor	X		X			

Reasons to choose STRIDE:

1.Comprehensive Threat Coverage: STRIDE provides a comprehensive framework that covers six major threat categories. This ensures that a wide range of potential risks and vulnerabilities specific to the Electronic Health Records (EHR) system can be identified and addressed.\\

2.Systematic Analysis: STRIDE offers a systematic approach to analyzing each threat category individually. This allows for a focused assessment of potential vulnerabilities and helps ensure that no major threats are overlooked. The systematic analysis helps in identifying specific weaknesses and designing targeted countermeasures.\\

3.Applicability to Healthcare Industry: The STRIDE method aligns well with the specific security requirements of the healthcare industry. It addresses the unique challenges faced by EHR systems, such as protecting patient privacy, ensuring data integrity, and maintaining the confidentiality and availability of healthcare information.\\

4.Countermeasure Selection: STRIDE not only identifies threats but also guides the selection and implementation of appropriate countermeasures. By analyzing each threat category, organizations can develop targeted security measures and risk mitigation strategies. This allows for a focused approach in enhancing the overall security posture of the EHR system.\\

By researching we got to know STRIDE also has **cons,**

1.Complexity: The STRIDE method can be relatively complex, it requires a good understanding of the EHR system's architecture, potential threats, and associated vulnerabilities.\\

2.Time and Resource Intensive: Conducting a thorough analysis using the STRIDE method can be time-consuming and resource-intensive.\\

3.Subjectivity in Risk Assessment: The process of assigning risk scores or prioritizing threats in STRIDE involves a degree of subjectivity.\\

OTHER ALTERNATIVE METHOD:

Other than the STRIDE method **OCTAVE** also is effective for the EHR system. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation):
OCTAVE is a risk-based methodology developed by the Carnegie Mellon University Software Engineering Institute. It focuses on identifying and prioritizing risks to critical assets within an organization. OCTAVE consists of three phases: build asset-based threat profiles, identify and assess vulnerabilities, and develop risk mitigation strategies.\\