

## Question 2

### Introduction

Cybersecurity is a very important factor for healthcare enterprises, as a data leak could release sensitive patient information into the world and GDPR strongly imposes protection on patient data.

When storing this information in the cloud, YorKlinik must put special care into ensuring that it is kept secure, but thankfully AWS provides a wide array of tools to aid this process.

However, even though AWS is very powerful it is also designed for large-scale enterprises, and the overhead this causes might conflict with YorKlinik's intention to stay lean.

Points:

- AWS security tools  
AWS provides tools for database management and encryption through RDS - relational database system.
- YorKlinik's capabilities
  - Development team  
As a small company, the development team of YorKlinik might be limited in resources, and they may resort to COTS (commercial off-the-shelf) solutions for ensuring security. These may not be verified or might not work with the security model required for medical data, which could be a large threat.
  - Entire company implications  
To bolster security and minimize the risk of attacks, YorKlinik will have to establish security protocols that will encompass everyone in the company. Because the medical data will need to be accessed often **citation needed**, measures need to be taken to ensure secure access and proper handling of the data. As the data is stored on a cloud server, it is of utmost importance that the access credentials are not intercepted.
- Challenges for a small-scale company working in an enterprise-scale security model  
AWS is an enterprise-scale service which accommodates small-scale companies, but this does not come without costs. Encryption of all data will be required but introduces an overhead in storing and retrieving the data, which is worsened by the fact that it is all stored off-site. However, this also reduces the risk when compared to

storing the data on-site, where a physical threat is more likely and attackers would have more ready access to the infrastructure.