Question 2

Using the cloud instead of an in-house datacenter is a great way of saving costs for a small business, but it does not come without its costs. There are severe security concerns around storing data in the cloud, which are intensified by the fact that medical data is confidential and a data breach would be a very serious issue.

For secure environments, AWS provides the Amazon Virtual Private Cloud (VPC), which allows users to define a logically isolated environment in which to run their applications [3]. Together with Amazon RDS (Relational Database System), it can be used to store data securely in the cloud [2]. This would be a perfect fit for the YorKlinic development team, who require these features to minimize the risk of a data breach and would otherwise have to implement them themselves, which would be a very large resource drain.

However, the development team would need to have both good security knowledge and practices to ensure that the data is kept securely. This would require the team to spend more time on security instead of development, which could be a drain on YorKlinic's resources [1].

By using AWS instead of an in-house datacenter, YorKlinic will not have to spend resources on securing their hardware and can instead delegate this onto Amazon, who have more resources available to ensure security. Amazon's customer service can also provide assistance with any issues that would otherwise need to be tackled alone.

However, this comes with the disadvantage that YorKlinic would be trusting Amazon to keep the data secure, as any hardware issue could potentially leak data and this is completely out of YorKlinic's control. In addition, in the event that a data breach did happen, it might be impossible to hold Amazon accountable due to current legislation [5].

Another disadvantage is that online data is by nature more vulnerable than data stored on site, and thus it might be easier for an attacker to find a way to breach security. Since AWS has had data breaches in the past [4], it is clear that using their inbuilt security features is not enough, and additional care has to be put into security.

In conclusion, as long as YorKlinic has the resources to ensure that proper security practices are followed, AWS can provide superior security

to what the startup could muster on their own. When used correctly, AWS can provide more security than an in-house datacenter could, as it allows YorKlinic to make use of their more secure infrastructure and wide range of security tools.