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. However, when used correctly AWS can provide more security than an in-house datacenter could.

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 [2]. Together with Amazon RDS - relational database system, it can be used to store data securely in the cloud [1]. This would be a perfect fit for the YorKlinic development team, who require these features to minimize the risk of a data breach.

However, the development team would need to have both good security knowledge and practices to ensure that the data is indeed 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. **Extend this**

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, a reputable, much larger company with many more resources to spend on security. Amazon's customer service can also provide assistance with any issues that would otherwise need to be tackled alone.

A major disadvantage of keeping data in the cloud is 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 find out where the data was compromised [4].

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. AWS has had data breaches in the past [3], and if large companies storing sensitive resources can have security issues it is likely that securing the data is not trivial.