1. To keep your data safe, various security levels are deployed like physical security (CCTV)

, network security (firewall), storage level security

All these strategies are employed to make sure the data is kept safe

1. Using proper authentication and authorisation we ensure data belonging to a particular use is visible only to him. Also, VM isolation is established, which means other customers can’t access your resources even if they are using the same hardware
2. To steal data, one requires credentials and respective accessing policies. To give a secure authentication, two factor authentication can be used where one will have to prove their identity twice in two different stages. Also, physical security can be provided such as CCTV surveillance, disabling few of the parts etc. To secure data at network level, firewall or de-militarized zone can be used
3. We have CISCO’s network security certification since to public health services too, we follow the HIPAA guidelines as well
4. On premises security is at par with the cloud security. The servers suarded by guards 24\*7 with camera surveillance. The door to the server room has a multifactor authentication system and requires a key card, a fingerprint and a passcode to open it. If anyone except authorized or serves room, alarm would go off and the person will be apprehended