**Risk Management**

Maintaining and disposing data is on par with the challenge involving data collection since the volunteers that have participated in data collection have been assured of their privacy. Which is why in order to increase volunteers' level of confidence, the data collection system must outline the aspects of the privacy policies. It includes not only the sensitiveness of data management but also immunity from hackers and malware. Therefore, firewalls and other layers of security in form of cryptographic data encapsulation are necessary for these systems. It is common to come across project management issues as they involve protocols that can also be improved upon by didn’t of SDLC waterfall agile methodologies. As opposed to FTP based CRUDE interface, the UI should be well designed and ergonomic. The cloud storage protection is one among many important factors. The data protection is a paramount concern. The cloud services policies from their providers should be thoroughly examined, and the data in their cloud servers must be well encrypted. Issues regarding UI can be major prominence. Users may experience issues while data transfers and the network concerns might result in no backup or backlogs. Cloud handlers' data labeling and integration imply risks such as data corruption while transmitting data to the labeler, in which cases there are risks of recording the video again. Backing up the raw data is the best strategy to mitigate the risk. In order to protect the users from the risk, firewall installation will be a crucial part of our contract with the cloud provider.