

mVisum[®] System Security



mVisum's security architecture is based on encrypted data running within an encrypted pipeline, each layer being independently capable of meeting HIPAA requirements. The mVisum server, located within the facility's firewall authenticates the user logging into the physician smartphone application and provides for SSL. User login on the physician smartphone is authenticated on the mVisum server using unique usernames and passwords, along with the phone number and/or the IMEI number of the device. The server also separates out the patient identifier (demographics) and the raw clinical data, and encrypts them separately. The physician smartphone contains the keys to decrypt these separate files and put them together into a patient file.

The patient data is resident on the mVisum server either until the conversation is "closed" by the console user (not shown), or times out. This time-out period for data on the server can be configured per the facility's requirements. The data on the smartphone can be set up to be erased each time the physician logs out, thus guarding against device theft. Further, if no activity is seen for a pre-defined time length, the handheld application automatically logs out.

