uArrive
CHECK-IN

Software Security:

OTech software is HIPAA compliant with a time out feature, quit option, password protected database, encrypted data transmission and stringent settings on memory and data storage.

Minimal Bandwidth Requirements

The kiosk is a client based computer, but the bandwidth required to communicate is very minimal. For queries and updates, the data transmitted is approximately 1 or 2 kilobytes. When a scanned insurance card image or signed authorization form is saved it is between 50 to 100 kilobytes. Form transmission depends on the file size of the PDF itself.

Application

OTech software is client based and integrated directly with the PMS database server. The application starts when the kiosk boots up in the morning and shuts down at the end of the day based on a configuration setting. The configuration data and logs are retained in a SQL Server CE database file that is password protected and encrypted. The log files can be purged after XX number of days (based on client preference).

Since the application could allow a patient to enter his/her social security number or name/DOB as a means of checking in, the year of birth and first 5 characters of the social security number are masked.

A time out feature that returns the application to the opening welcome screen and a “QUIT” button on each screen protects patient data should the patient terminate the check-in session.

After a patient completes or aborts a check-in, the data that is either read from the driver’s license or the practice management system are erased from memory.

A utility continually checks to see that the application is running. If not, it forces a reboot of the system to prevent anyone from trying to hook up a keyboard and access any information on the computer.

Protected Health Information

The application maintains limited data in its logs and masks things such as year of birth and or partial social security numbers. The data resides in a password protected/encrypted database and can be purged at regular intervals (based on client preference).

PCI Compliance

All credit card transactions are processed using a secure and encrypted PCI compliant means of communication. Card information is not stored on the kiosk.