

## Bringing Mobility to Healthcare

The mVisum Medical Communication Platform is a software solution that facilitates secure and rapid transmission of patient data to mobile devices.

- ✓ **Client based application (Not a slow website!)**
- ✓ **Secure - HIPAA Compliant**
- ✓ **Fast data transfer**
- ✓ **Works with existing infrastructure**

mVisum technology permits the rapid transmission of complex data such as:

- ✓ **EKG's**
- ✓ **Echocardiograms**
- ✓ **Cine Loops**
- ✓ **Ultrasound movies**
- ✓ **Waveforms**
- ✓ **MRI's**
- ✓ **CT Scans**
- ✓ **X-Rays**
- ✓ **Alarms**
- ✓ **Laboratory Results ...and more !**



## Device Compatibility

The mVisum Medical Communication System is compatible with the following smartphone types\*:

- **Blackberry** (8300 series and later)
- **Android**
- **iPhone** (v2.2.1 or later)
- **Windows Mobile**

*\*Please refer to our Hardware Requirements document found on our website for complete specifications.*



## Security and HIPAA Compliance

mVisum push delivers data to mobile devices from various clinical data sources (e.g. PACS systems, EKG archives, EMRs, etc.) in a fully secure and traceable manner that meets or exceeds HIPAA requirements.

**Traceability:** All key aspects of message transmission, delivery, and review are fully traceable. Each message is fully traceable from the point of receipt at the mVisum server, availability on server for physician, physician message receipt, review, and response.

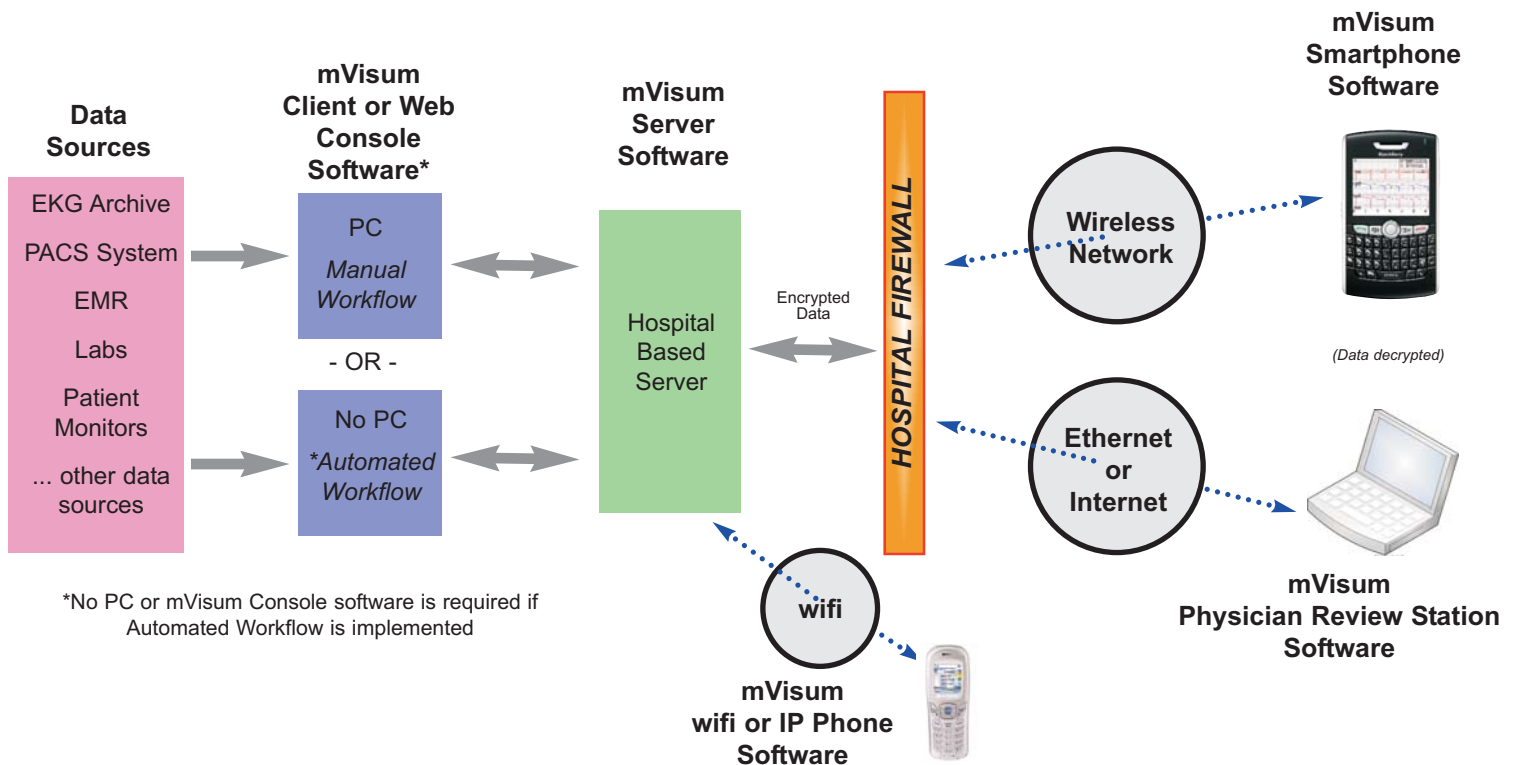
**Reporting:** QA and other reports pertaining to any aspect of message creation, delivery, or response are configurable.

**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, effectively providing data security above and beyond HIPAA requirements. The physician smartphone contains the private keys to decrypt these separate files and put them together into a patient file. mVisum employs a secure 128 bit encrypted data pathway.

**User Management:** All user accounts can be remotely deactivated and the user forced to log out.

**Auto-logout/temporary data:** The handheld software resident on the smartphone has auto-logout features that automatically log out after pre-specified time periods. On manual or auto-logout, any and all patient data-downloaded is removed from the device hence further reducing any risk of device loss.

## The mVisum Process at a Glance



**mVisum, Inc.**

Waterfront Technology Center  
200 Federal Street, Suite 230  
Camden, NJ 08103

Phone: 866-mvisum1  
email: info@mvisum.com  
web: [www.mvisum.com](http://www.mvisum.com)