Introduction

As the reliance on healthcare data grows, the inter-connectivity and regulatory governance of these devices plays a vital role in patient monitoring, clinical decision support, and care.
The following are solutions to four challenges medical device original equipment manufacturers (OEMs) will face as they prepare for the future of connected care.

Source: Phani Bidarahalli, General Manager and Head of Healthcare & Life Sciences, Wipro's Product Engineering Services http://www.t-odaysmedicaldevelopments.com/article/4-steps-to-connected-healt-hcare/

1. Accurate timing

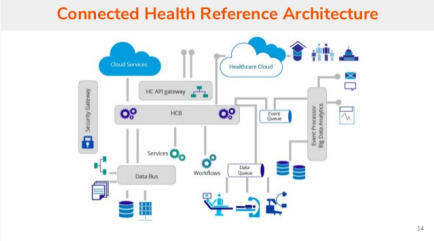
As primitive at it may seem, the biggest debate today in the medical world is: What is the correct time? Is it the time on the wall clock, the time on the device, or the time on the doctor's watch? Timestamping measured data is crucial, as caregivers working across devices need to know what type of care was given to a patient and exactly when. To meet that need, caregivers cannot go by a nurse's recording of time from a wall clock. Devices must recognize the Network Time Protocal (NTP) of outside devices and synchronize device time to server time. Designers should never assume the internal clock on their device will be the only source of time..

2. Eliminate user actions

The less time a caregiver spends manually using or entering data into a device the better. Avoiding proprietary workflow issues can eliminate the probability of human error. Devices should be designed to perform data exchanges as independently as possible without the need for user intervention. Designers also need to recognize and understand the broader setting where a device will be used.

For example, the requirements of a device in a cardiac care center can vary from the requirements of the same device in an orthopedic setting. Research and development teams that connect medical device OEMs with usability experts and clinicians can improve workflow.

Connected Healthcare



3. Secure pairing

Technology such as Bluetooth can present challenges in pairing and un-pairing devices, potentially causing data loss and unsecure communication. Designers must understand pairing needs of individual devices. Arbitrarily pairing devices could expose patients to non-standardized information. If a nurse wants to send a prescription to an infusion device, the infusion device and the device sending the prescription need to have a perfect handshake so the source can be authenticated. This could prevent a nurse from accidentally delivering a prescription to the wrong device. Medical device OEMs need to adopt secure public and private key encryption mechanisms and institute design and audit processes that frequently monitor data loss..

4. Managing compliance

Health Insurance Portability and Accountability Act (HIPPA) compliance is an area of concern for medical device manufacturers. As more and more technology manufacturers embrace open source technologies and commercial libraries available for data encryption, it is important to understand how those technologies will impact HIPPA compliance. Medical device designers must understand the trail of data that could potentially be left on another device and should conduct accessibility testing of open source packages to ensure they are securing patient records and data to meet HIPPA requirements..