Mobility in healthcare: The glass half-empty view

Mobility has shaken up healthcare to the point where conventional care delivery no longer suffices. The use of smartphones and tablets in hospitals has made it possible to deliver medical records straight into the hands of doctors and healthcare team members. When tasks are organized and workflow is streamlined healthcare professionals spend less time on administrative duties and more time taking care of the patients.
But, is that enough to go all in on healthcare? Recent reports on healthcare data breaches alone suggest not.

Some alarming facts and stats

According to an Identity Theft Resource Centre (ITRC) report, Healthcare industry contributes 43 percent of all the data breaches identified in 2014. What attracts cybercriminals to healthcare is the ease with which they can find individuals' personal information, Protected Health Information (PHI) and credit card information in one place. Reuters reckons, one's medical information is worth ten times more than the credit card information. Stolen credit cards tend to be canceled immediately by the bank but medical identity thefts are not usually identified promptly. Hence, criminals can continue to exploit their credentials for years.

Black market sale of data includes names, birth dates, addresses, social security numbers, insurance policy numbers, diagnosis codes, and billing information. Fraudsters can use these data to fake medical records and raise fraudulent insurance claims. Personal information can be used for creating fake IDs to buy drugs or expensive medical equipment. Either way victims end up with maxed out insurance benefits and wrong medical profiles. False medical history can have devastating health implications and may even be fatal. Confidential medical records ending up on the internet can make a patient's life living hell. It is estimated that the potential cost of data breaches in the healthcare industry could be a staggering $5.6 billion annually.

The challenges

Outdated legacy systems with hospitals and healthcare providers make things easy for hackers. These organizations often don’t have the technology or resources to deal with the data breaches. Add smartphones and tablets into such an environment already crippled with serious challenges and everything goes haywire. For the Healthcare industry, there is no shortage of policies and legislations, proper implementation is what it lacks of. Any mobile device that transmits, receives or stores Protected Health Information (PHI) comes under the Health Insurance Portability and Accountability Act of 1996 or HIPAA. The HIPAA Ominbus rule and the HITECH act further strengthen the security and privacy regulations for PHI in electronic form. Complying with these regulations not only saves organizations hefty fines but also prevents damage to reputation and customer trust.

Healthcare providers and hospitals need to form a clear organization-wide mobility strategy before deploying mobile devices or allowing BYOD. A formal risk analysis need to be carried out to assess the effectiveness of the security measures in place. A strong disaster management plan makes sure organizations can suitably respond to malware outbreaks and data breaches. Mobility in itself is demanding, what matters is how well healthcare organizations are prepared to meet the challenges it throws their way.