The Cure for Common Smartphone Ailments in Healthcare

spectralink
The WorkSmart Company

A SPECTRALINK WHITE PAPER

Eighty-nine percent of hospitals interviewed expressed concerns that consumer grade smartphones were not well suited for a hospital-based environment due to durability, usability and sterility concerns.

Introduction

With the passage of the Affordable Care Act, hospitals are facing stringent readmission penalties, patient-centered care models and financial incentives focused on patient safety, satisfaction and outcomes. At the same time they are tasked with treating an unprecedented influx of new patients – often engaging with multiple medical specialties. At the front lines of this healthcare evolution is the nursing community.

According to a recent report by Spyglass Consulting Group, *Healthcare without Bounds, Point of Care Communications for Nursing,* nurses are the single largest healthcare professional group in the United States, with approximately 2.9 million members. Facing constant pressure to communicate, collaborate and coordinate across a wide array of team members, nurses often rely on their own personal mobile devices (i.e., smartphones and tablets), to eliminate communication bottlenecks, streamline productivity and deliver improved patient care.

While the bring-your-own-device (BYOD) movement has promoted the use of employee-owned mobile devices to achieve greater productivity and cost savings, many healthcare organizations lack a mobile governance strategy. According to the Spyglass report, a stunning seventy-eight percent of hospitals interviewed didn't have a comprehensive mobile governance strategy outlining mobile usage policies. And seventy-three percent of hospitals interviewed lacked dedicated help desk personnel to support mobile end users.

Eighty-nine percent of hospitals interviewed expressed concerns that consumer grade smartphones were not well suited for a hospital-based environment due to durability, usability and sterility concerns. Yet sixty-seven percent report that staff nurses are using personal smartphones to support clinical communications.

Despite growing acceptance, hospitals often realize too late that **not all smartphones are created equal**, and actually can't withstand the rigors of 24/7 use. Furthermore, there are a limited number of enterprise-class smartphone solutions available that provide the following:

- Real-time VoIP communications
- HIPAA-compliant secure text messaging
- FDA approved alert and alarm management
- Simple nursing documentation (i.e., vital signs/IO, pain scores, etc.)
- Bar coding medication administration

This white paper addresses common consumer smartphone ailments as well as five key areas that healthcare organizations should consider before adopting a BYOD policy with consumer grade smartphones in the workplace.

1. Privacy, security and compliance
2. Integration and management
3. Call and phone quality
4. User distraction and patient safety
5. Total cost of ownership (TCO)

Privacy, security and compliance

The recent wave of breaches experienced by healthcare giants such as Anthem and Blue Cross Blue Shield has healthcare organizations focusing more attention on security and compliance than ever before. However according to recent research from the Ponemon Institute, forty-eight percent of healthcare IT and IT security practitioners said their organization had a breach involving loss or exposure of patient information in the past year. One of the biggest threats they face is unsecured mobile devices.

Despite growing cybersecurity threats against healthcare organizations, many continue to struggle with lack of resources. According to research by HIMSS Analytics and Symantec Corp., more than half of healthcare organizations surveyed allocate three percent or less of their total IT budget to security. Most organizations conduct security risk assessments just once a year, and only twenty-three percent have an ongoing, consistent risk management program.

IT needs to have visibility and control into the data being stored on the mobile devices used by workers. This visibility is critical for achieving and maintaining HIPAA compliance. HIPAA regulations require that healthcare organizations maintain detailed audit logs that provide an "electronic book of evidence" of their compliance activities. This information includes user information, location, IP address, types of devices (e.g. smartphone, tablet or laptop), URL accessed and any other pertinent details. If a device is misplaced or stolen, IT can leverage that information to produce a list of all the data stored on that device and evaluate the risk associated with the loss.

Smartphones are also easily stolen and are a favorite target of thieves. **It takes less than half an hour to crack a typical four-digit security passcode found on a smartphone.** This leaves healthcare IT managers with little time to remotely access and/or wipe sensitive data from a phone, if the phone has that feature.

Integration and management

Eighty-seven percent of hospitals interviewed expressed concerns about the costs, complexities and resources required to integrate consumer grade applications with the hospital infrastructure. And that sound you just heard is a sigh of relief from thousands of health IT teams that need to manage these infrastructures.

HIPAA requires that protected health information (PHI) such as patient names, social security numbers and so forth not be downloaded to unsecured, personal devices. A healthcare organization's IT team must be able to block and control critical information before it is downloaded to BYOD devices via a set of pre-determined rules that detect and recognize PHI.

IT also needs visibility into what happens with sensitive corporate data after it has been downloaded to an employee's BYOD device. Specifically, IT needs to keep tabs on where that data travels, and be able to gauge the sensitivity of that data. Visibility via such activities such as transaction logging and alerts can be a means of deterring employees from accidentally or deliberately disseminating sensitive information outside the organization without authorization.

However, as one director of clinical systems at a community hospital put it, "Hospital IT does not have the appetite to integrate, test, support and maintain consumer grade software to run securely in a highly regulated environment due to limited resources, systems integration complexities, and potential security threats."

Eighty percent of hospitals indicated that nurses were exchanging unsecured text messages that included patient health information.

Call and phone quality

One of the biggest challenges hospitals face when deploying personal smartphones within in-building work environments is delivering acceptable voice quality when leveraging organizations' in-building Wi-Fi network. Smartphones are primarily designed for cellular voice calls and data. Most smartphones also support Wi-Fi functionality. However, this support is optimized for data, not voice, and most smartphones are typically missing key features such as Quality of Service (QoS) support for prioritizing voice packets. Voice has a very low tolerance for network errors and delays. Gaps of only a few hundred milliseconds will deteriorate voice quality.

Not surprisingly, many hospitals face cost pressures which prevent them from making investments to improve cellular coverage. And as one chief medical officer noted, "Cellular coverage remains spotty throughout many of our buildings, especially on the lower floors where there are lined rooms within the Radiology departments and operating rooms. Improving cellular coverage is dependent (in part) upon the local wireless carriers' willingness to reposition local towers and antennas."

User distraction and patient safety

The personal use of mobile devices while at work can hinder productivity and cause risks to patient safety. Text messages, social media and personal phone calls expose nurses and other caregivers to distractions, taking their attention away from the task at hand. Sensitive data is another issue with smartphones. For example, smartphone features could potentially allow the violation of patient privacy by sharing photographs.

The reality of cell phone distractions impacting patient care attracted national attention in 2011. According to recent article in The Atlantic entitled, "Texting from the Operating Room," a Texas anesthesiologist was accused of sending text messages and emails while monitoring a patient. Her oxygen levels dropped, which the anesthesiologist didn't notice for close to 20 minutes, and she died in surgery. The women's family sued the anesthesiologist, ultimately settling the case before it went to trial.

Total Cost of Ownership (TCO)

While implementing a BYOD policy seems like a smart, cost-efficient move, there are several hidden costs, including lack of durability, the potential for theft, additional support requirements and investments in accessories required to make a consumer grade smartphone suitable for use in a healthcare environment.

Organizations often view the expense of deploying consumer grade smartphones only in terms of initial procurement costs, and often don't consider the total cost of owning a smartphone over its lifetime of usage. Replacement costs due to smartphones being damaged, lost or stolen can also greatly impact an organization's IT budget.

In order to maintain employee productivity, healthcare organizations must ensure that replacement phones are always available to swap out for any devices that are out of use. This generally means stocking extra phones to replace those out of service due to battery recharging, or those that have failed due to damage from dropping, shock, dust, or moisture Battery chargers and extra batteries add to an organization's bottom line – although some smartphones are sealed units that do not enable battery replacements.

Durability and sterility must also be considered. Most consumer grade smartphones can't withstand the typical bumps and drops that occur during normal use in healthcare environments. These phones are also not easily cleaned or disinfected. Standard hospital cleaning agents capable of killing hospital "Super Bugs" can damage the screen, casing and/or internal electronics of a standard consumer smartphone. Protective cases or sleds can provide additional durability protection for consumer grade devices, adding to the cost.

In 2012, the ECRI Institute, a non-profit that focuses on healthcare quality, listed cell phone distraction among the top 10 risks that can impact patient safety.

Consumer smartphones usually have short lifecycles, often measured in months, before a new and "improved" version is available. Frequently these changes are minor features that have no bearing on improving employee productivity. However, replacing like-for-like phones can be impossible if older versions have been discontinued. Newer versions of devices may have different form factors or use different accessories, requiring additional unplanned investments.

Many smartphones have their own portfolio of after-market add-ons that can make a consumer smartphone highly customizable to particular uses and environments. These can add key functionality such as industrial barcode readers or magnetic card readers. But a large number of these add-ons can be made obsolete by a simple change of physical dimension or a phone's connector port.

Conclusion

As caregivers continue to rely on consumer smartphones, healthcare organizations must carefully weigh the benefits with additional costs, as well as impacts to security, compliance, patient care and safety. In most cases, clinical smartphones are specifically designed and tested for use in healthcare environments – outperforming smartphones in terms of durability, security and call quality, while ensuring security and compliance of sensitive patient data.

Purpose-built, in-building clinical smartphones are designed to meet the specific needs of mobile professionals in healthcare environments. Essential features in these smartphones include excellent voice over in-building Wi-Fi and DECT wireless networks, extensive battery life with long talk time and/or easily replaceable batteries, and ruggedized design to withstand bumps, drops and harsh cleaning agents. These smartphones differ greatly from consumer smartphones in several ways:

- They have significantly longer product lifecycles than consumer smartphones, resulting in a lower total cost of ownership
- They are designed for secure access and exchange of protected health information in accordance with HIPAA compliance
- They integrate with industry-specific workplace applications

Within healthcare environments, the benefits of deploying clinical smartphones outweigh those of consumer grade smartphones in terms of security and compliance of sensitive patient data, durability, call quality and total cost of ownership.

Clinical smartphones are specifically designed and tested for use in healthcare environments — outperforming consumer grade smartphones in terms of durability, security and call quality.

Information resources

Healthcare without Bounds, Point of Care Communications for Nursing
Spyglass Consulting Group | © March 2014

Fierce HealthIT – *Resource constraints hamper hospital cybersecurity efforts*
March 1, 2016 | by Susan D. Hall

Fierce HealthIT – *Report: Healthcare cyberattacks occur almost monthly*
March 2, 2016 | by Susan D. Hall

The Atlantic – *Texting from the Operating Room*
July 20, 2015 | by Shefali Luthra

About Spectralink

Spectralink delivers secure, cost-effective mobile communication solutions that empower enterprises to streamline operations, increase their revenues and deliver a positive customer experience – each and every time. Since 1990, Spectralink has deployed millions of devices worldwide across the retail, healthcare, hospitality and manufacturing sectors – providing workers with the industry's most efficient, in-building communications. Visit www.spectralink.com for more information.

Spectralink
2560 55th Street
Boulder, CO 80301
Tel: +1 800 775 5330
info@spectralink.com
spectralink.com