Secure Mobile Communications in the Healthcare Industry:

Supporting New Healthcare Delivery Models

FROST & SULLIVAN

A Frost & Sullivan White Paper

contents

INTRODUCTION AND OVERVIEW

This Frost & Sullivan market insight report presents an overview of secure mobile communication solutions used in healthcare facilities within the United States. It highlights key success factors for secure mobile communication solution providers and offers strategic recommendations for hospitals that want to implement a secure mobile communication solution. Throughout this report, "secure mobile communication solution" implies a smartphone-based mobile communication device that allows secure voice, text, images, and video-based communication between hospital staff members, extended staff, and physician groups outside the hospital. It also supports information exchange between hospital IT systems and smartphones.

SECURE MOBILE COMMUNICATION IN HEALTHCARE

Despite the rise of mobile applications and BYOD (bring your own device), many healthcare organizations still rely on antiquated systems such as pagers, faxes, and paper-based records to communicate and collaborate, or they use applications that do not extend across sites. Using inefficient systems and processes for care coordination and other important functions in hospitals can negatively impact patient care, safety, satisfaction and outcomes. Today's mobile computing platforms present a powerful set of capabilities for hospitals and health systems that, if leveraged properly, can improve care team collaboration and the efficiency of day-to-day operations. Realizing this value, many hospitals have implemented secure mobile communication solutions for mission-critical communications. Changes in federal healthcare regulations that incentivize healthcare facilities to deliver improved patient care, facilitate better data and image sharing, and focus on improving patient satisfaction levels are driving a shift toward open, extensible, interoperable, and "mobile-compatible" communication systems that expand across sites in the U.S.

Secure Mobile Communication—Trends

Smartphones are becoming smaller and more powerful with greater healthcare-relevant options, such as secure voice and data communication, remote device management, and mobile applications that can access or use important healthcare IT systems. This capability enables support for a wide range of healthcare use cases, including seamless care coordination, physician alerts, and patient engagement. However, personal smartphones cannot simply be brought into hospitals and used "as-is." A significant amount of customization, integration, and security enhancements are required to make smartphones compliant and usable in hospital environments. Additionally, not all secure messaging applications work across sites or with other applications, exacerbating communication silos and increasing complexity when using multiple applications. This is why enterprise-grade, secure mobile communication solution providers are needed. Enterprise, secure mobile solution providers use on-premise (e.g., servers are bought and maintained within a local data center) or a combination of the two or cloud-based platforms (e.g., data is stored in a hosted data center managed by another company in a different location) to deliver clinically relevant (and secure) voice and/or data communication services that improve clinical workflow and ultimately deliver better patient care at a lower cost. Some key trends driving smartphone adoption in hospitals include:

- **Bring your own device (BYOD):** Mobile devices have transformed the way business is conducted today. An increasing number of U.S. businesses are deploying mobile software applications for use by their employees. A similar trend is starting to appear in the healthcare industry as well, where physicians and nurses are increasingly demanding access to work-related IT applications on their personal mobile

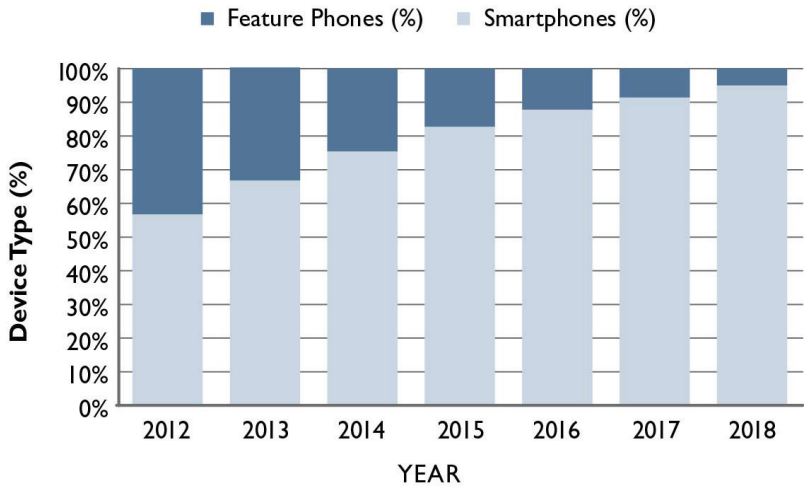
devices. As a result, there is a proliferation of applications, and hospitals are exploring ways to provide their workforce with secure mobile access on their personal mobile devices in the form of BYOD, or are providing institution-owned mobile devices.

- **Increased device security:** The current generation of smartphones support advanced data protection mechanisms, including multiple levels of user validation, encryption and authentication, and support for digital certificates. These technologies can be used to comply with the strict data privacy requirements of hospitals.

- **Support for multiple communications and data-sharing methods:** Solution providers can leverage text messaging, email, hands free devices, and other tools for deploying for deploying secure mobile communication solutions. This capability helps mobilize multiple types of clinical data sets in a format most suited for the recipient device.

- **Availability of robust and secure on-premise, cloud and/or hybrid services:** On-premise software deployments are popular in hospitals, given security requirements. However, cloud-based platforms are making strong inroads in healthcare, and their adoption (as well as adoption of hybrid models) is expected to increase in the next five years. Research indicates that it is not only the size of the organization that decides if an organization chooses an on-premise, hybrid or a cloud-based platform. Factors such as ease of implementation, integration with key hospital systems, total cost of ownership (TCO), return on investment (ROI), and product capabilities also play an important role in this decision.

Exhibit 1 shows the evolution from feature phones to smartphones in the U.S. from 2012 to 2018.



Note: All figures are rounded. The base year is 2013. Source: Frost & Sullivan

Exhibit 2 shows key trends in enterprise mobile application adoption in the U.S.

Percent of North American businesses that have currently deployed mobile application to at least some degree		Percent of North American businesses that plan to introduce or expand mobile application deployment within the next 3 years	
62%	Wireless email	49%	Wireless email
39%	Access to internal corporate database(s)	46%	Access to internal corporate database(s)
32%	Standalone corporate instant messaging	45%	Mobile workforce management
32%	Employee-to-employee social media	40%	Mobile sales force automation
31%	Mobile sales force automation	39%	Standalone corporate instant messaging
30%	Mobile workforce management	38%	Mobile asset tracking
27%	Mobile asset tracking	38%	Employee-to-employee social media
24%	Mobile supply chain management	37%	M2M remote monitoring and diagnostics
23%	M2M remote monitoring and diagnostics	37%	Mobile supply chain management
23%	Standalone video capture	34%	Fleet tracking and management
20%	Fleet tracking and management	33%	Standalone video capture

Source: 2013 Mobile Enterprise Applications Survey Design and Coverage; Frost & Sullivan

Secure Mobile Communication—Demand Drivers

The key demand drivers for smartphone adoption in hospitals include:

- **Need to address communication inefficiencies:** By allowing information to be pushed to the responsible or designated staff member in the hospital, smartphones can address many existing communication challenges when selecting an enterprise-grade solution. For example, workers in a hospital don't have to spend time on unproductive activities (such as walking down hospital hallways to track down the attending physician). They can use an enterprise-grade smartphone solution that includes multiple functionalities and can be used across sites to call or send a text message to the physician in charge. Similarly, critical lab results could be sent via secure messages to the on-call physician, who can then respond appropriately. A simple use case such as being able to quickly communicate with designated staff members who are on duty can collectively save hundreds of thousands of minutes for a single, large hospital every year. This speaks volumes about the potential of secure mobile communication solutions.

- **Federal mandates:** Federal directives encourage hospitals to adopt advanced IT systems and technologies to improve the care experience. For example, Medicare and Medicaid Electronic Health Records (EHR) Incentive Programs provide financial incentives for the "meaningful use" of certified EHR technology. As stated on the federal government website, cms.gov, to receive an EHR incentive payment, eligible providers must prove they are "meaningfully using" their certified EHR technology by meeting certain measurement thresholds that range from recording patient information as structured data to exchanging summary care records. These developments have led to an increased adoption of digital healthcare IT platforms. In other words, mobile health technology has emerged as a natural extension of the new generation of healthcare systems and IT platforms that are in various stages of implementation throughout the country. Selecting a secure messaging solution that can help meet these federal mandates by integrating IT platforms while connecting all members of the patient care team is critical.

- **Emergence of performance-based and success-linked models in healthcare:** The emergence of the Accountable Care Organization (ACO) model makes it important to ensure quality, appropriateness, and efficiency of healthcare provided to patients across the full continuum of care. Numerous studies have identified communication inefficiencies and lack of proper data sharing as major hurdles in offering a truly patient-centric service delivery model. The healthcare industry is already moving in the right direction by adopting EHRs and other standards-based data records management platforms—many of which can be integrated with smartphones to varying degrees of depth. A shift to a mobile-centric communication framework is expected to take time as many legacy platforms have complicated back-end systems that cannot be simply updated to ensure data is transferred and displayed properly and securely on mobile devices.

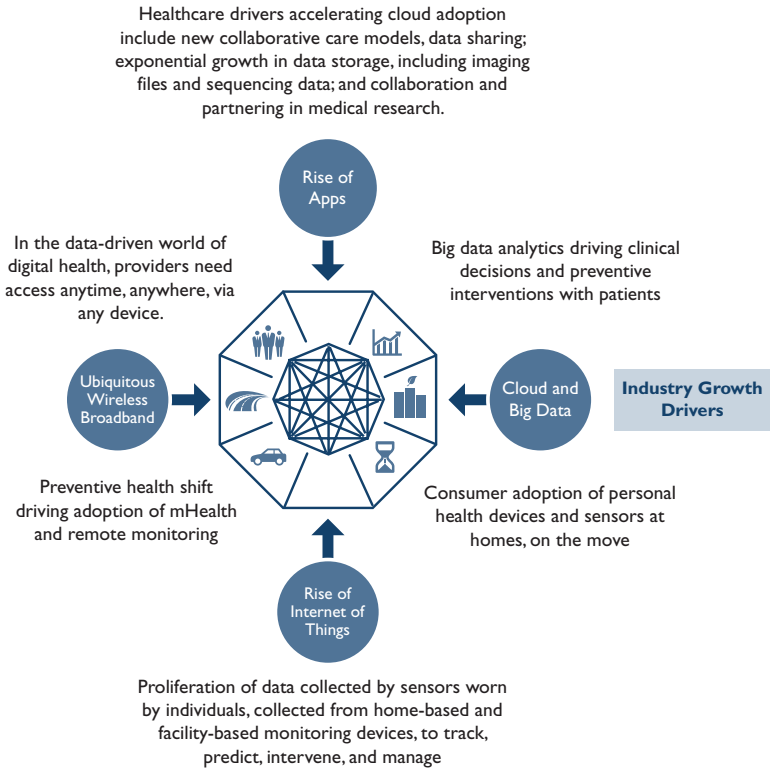
- **Pager replacement:** Smartphones are the leading candidate for pager replacement. The current set of secure mobile communication solutions support multiple directories and are multi-site-capable, which allows healthcare professionals who work at multiple facilities to carry a single device for their remote communication. Additionally, solutions that allow a message to be delivered simultaneously to a pager and to a smartphone further help support the case for smartphones in hospitals.

- **Preventing privacy violations:** Many healthcare professionals use common text messaging services such as Short Message Service (SMS) and Multi-media Messaging (MMS) to communicate with each other. These services are not only insecure—messages are sent in clear text and are not encrypted—they are also not suited for critical, time-sensitive communication as immediate delivery is not guaranteed. It is in the best interest of hospitals to implement protocols that allow doctors, nurses, and other staff to use their smartphones for quick, easy text-based communications in a secure and reliable manner. This trend is similar to the developments in other industries, where organizations realize that the cost of providing a secure way to communicate through smartphones is significantly lower than the potential costs of doing nothing.

- **Eliminating inefficiency across the continuum of care:** According to The Joint Commission[1], an estimated 80% of serious medical errors involve miscommunication between caregivers when patients are transferred between points in their care journey. In addition to patient harm, mishandled patient transfers can lead to delays in treatment, inappropriate treatment, and increased length of stay in the hospital. Technology-driven solutions that span the entire continuum of care—before admission, during treatment, and at discharge—and include all members of the care team regardless of location, device, or business relationship, ensures that excellent care coordination is delivered to patients throughout their "care service lifecycle." It is Frost & Sullivan's opinion that smartphones used in conjunction with other hands-free mobile devices are one of the best toolsets to ensure care teams remain in sync by providing seamless and continuous communication between healthcare providers and patients. This synergy is especially important in an era where care is delivered by more than one healthcare facility.

1 The Joint Commission is an independent, not-for-profit organization that accredits and certifies more than 20,000 healthcare organizations and programs in the U.S.

Exhibit 3 shows shifts in healthcare and information technology supporting the industry transformation in the U.S.



Source: Frost & Sullivan

Exhibit 4 shows the future of modern healthcare in the U.S. as it relates to secure mobile communications.

FROM		TO
Fragmented	Patient Flow	Integrated and Automated
Invasive	Diagnosis and Treatment	Less invasive, preventative, image-based
Provider-centered	Focus	Patient-centered
Hospital-centric care	Organization	Collaborative, multi-site model
One-size-fits-all	Approach	Personalized Medicine
Therapeutics/ Diagnostics/Devices	Tools	"Theranostics"
Treating Sickness	Objective	Preventing Sickness- "Wellness"

A modern healthcare system, demanding a healthcare paradigm shift, is on the horizon.

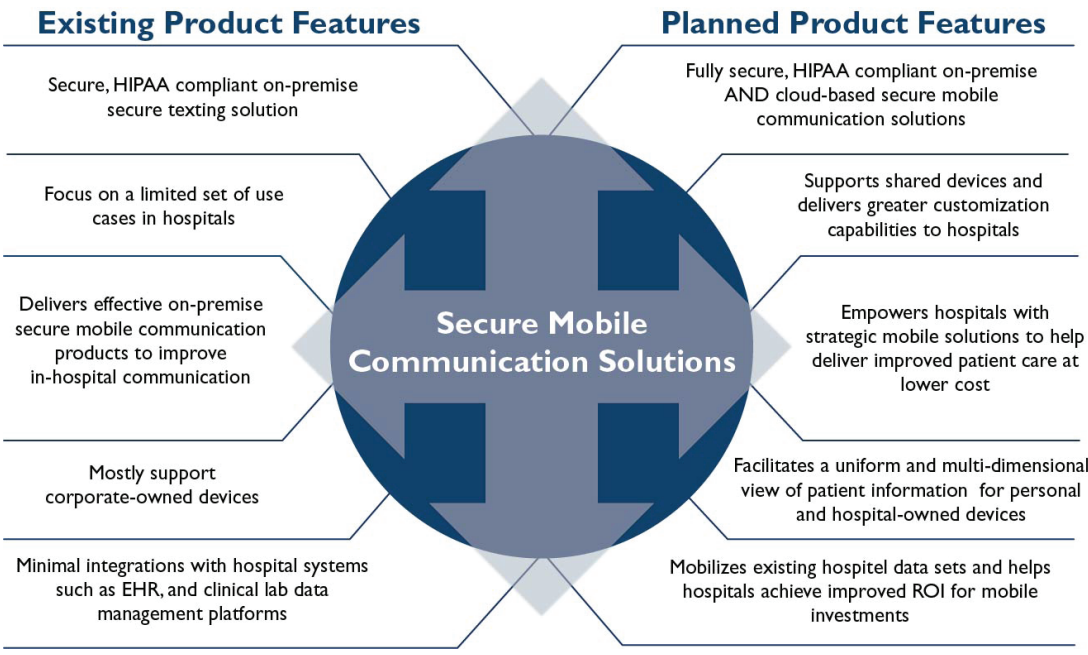
Source: Frost & Sullivan

Secure Mobile Communication—A Holistic Solution

It is somewhat limiting to define secure mobile communication solutions as implementations that only provide access to patient information or allow secure texting. Enterprise-grade smartphone solutions can also help improve clinical workflow, patient safety, satisfaction, and clinical outcomes. For example, according to Vocera, a provider of enterprise-grade communication solutions for life-critical mobile environments, their Collaboration Suite provides integrated functionality so that doctors, nurses and all members of the extended care team can communicate and collaborate in real-time. The real-time staff assignment directory ensures that the clinical team is able to remain in sync to improve workflow efficiencies both inside and outside the hospital; eliminating the need for multiple devices, searching for caregivers or hunting for lab data. This level of automation is achieved by integrating smartphones (through workflow and mobility management platforms deployed either in the cloud or on-site) with existing clinical IT systems and technologies.

In fact, leading secure mobile communication solution providers have varying abilities to integrate with IT systems such as EHRs, nurse call systems, patient monitoring, bed management systems, clinical lab data management platforms, real-time alert systems (RTLS), and asset tracking systems (such as radio frequency identification or RFID-based solutions) to provide relevant and timely information on appropriate personnel's mobile devices. This integration capability means that both person-to-person and machine-driven automated communication can be supported by smartphone-based secure mobile communication solutions.

Exhibit 5 shows existing and planned product features of smartphone-based secure mobile communication implementations in the U.S. healthcare market for 2014.



Source: Frost & Sullivan

HCAHPS AND SECURE MOBILE COMMUNICATION

The HCAHPS (Hospital Consumer Assessment of Healthcare Providers and Systems) survey is the first national, standardized, and publicly reported survey of patients' perspectives of hospital care. According to Centers for Medicare & Medicaid Services (CMS), the HCAHPS survey is designed to produce data about patients' perspectives of care that allow objective and meaningful comparisons of hospitals on topics that are important to consumers. CMS also believes that public reporting of survey results creates new incentives for hospitals to improve quality of care. The HCAHPS survey asks discharged patients 27 questions about their recent hospital stay. The survey contains 18 core questions about critical aspects of patients' hospital experiences, including communication with nurses and doctors, the responsiveness of hospital staff, the cleanliness and quietness of the hospital environment, pain management, communication about medicines, discharge information, overall rating of hospital, and if they would recommend the hospital.

Hospitals use HCAHPS survey results to track improvements in patient experiences. In fact, many leading hospitals have improved their HCAHPS scores by leveraging advanced communication and collaboration tools that help them deliver faster, better patient care—a clear validation for the use of next generation mobile communication and collaboration platforms in healthcare. For example, leading hospitals in the U.S. that have implemented advanced mobile technologies to streamline the communication process between nurses, physicians, and patients have witnessed improvements of nearly 20% in the HCAHPS domain related to inpatient perceptions of the quietness of the hospital environment. Similarly, many hospitals that have leveraged advanced mobile and wireless solutions for improved staff-to-staff communication have seen their HCAHPS responsiveness scores improve significantly within a few months of implementing the communication solution.

By using secure mobile communication solutions, hospitals can improve the patient experience in the following ways:

- Faster care delivery through better connected caregivers;
- Noise reduction (quietness of hospitals) through the reduction of overhead paging;
- Improved ability to respond to alarms when solutions are integrated with alarm systems;
- Reduced readmissions and fewer errors in patient care (through improved staff communication and more frequent rounding);
- Improved patient hand-offs when patients transition between clinical staff members or healthcare facilities; and
- Improved patient engagement and communication from pre-arrival to hospital discharge.

Ultimately, mobile solutions make communication more transparent, while improving care team coordination, work flow efficiency and the overall healthcare experience.

ALARM SAFETY ISSUES AND ROLE OF MOBILITY

Many different types of medical devices have alarm capabilities that can be used to notify clinical staff about the status — or changes in the health — of a patient under observation. However, rapid proliferation of alarm-enabled technologies, coupled with improper usage or lack of training, has resulted in a real alarm management problem for hospitals in the U.S. and around the world.

It is to the point where alarm hazards have been identified as one of the top healthcare technology challenges by the Emergency Care Research Institute (ECRI).[2] For example, ECRI studies show that the typical cardiac unit can experience as many as 12,000 alarms in a single shift, with each type of alarm having a different sound and different clinical response requirement. Together, these are key contributors to alarm fatigue.

According to The Joint Commission, between 85 to 90% of alarms may not need immediate (or any) clinical intervention and are simply generated when the alarm conditions are set too tight, default settings are not adjusted for individual patients, and machines are not maintained properly. This barrage of alarms (generated because of improper alarm settings, for example) has resulted in an industry problem called "alarm fatigue." There have been several known instances of genuine alarms not being attended to because of the clinical staff's tendency to either turn off the alarm volumes, or adjust the alarm settings outside the limits that are safe and appropriate for the patient—some of which have resulted in fatal consequences for patients.

To address alarm fatigue and related risks, many healthcare leaders are beginning to seek intelligent alarm management solutions that offer rich media-enabled alarm capabilities that can provide clinicians with detailed alarm information on their mobile devices beyond just a simple text-based notification. For example, delivering an alarm with an included image or relevant clinical data (such as an ECG waveform or vital signs) can allow the physician to determine the extent and level of the criticality of the alarm and make appropriate treatment decisions. Such smartphone-based alarm management solutions are positioned as secondary alarm notification systems that offer greater insight and allow caregivers to prioritize alarms based upon criticality of every alarm. Contextual alarm solutions are expected to emerge as an important feature set for secure mobile communication solution providers in the next three to five years.

ESSENTIAL FEATURE SETS AND SUCCESS FACTORS

Product capabilities, ease of deployment, system integration options (including EHR and alarms), user experience, customer support capabilities, go-to-market strategy (including partner relationships), and a strategic roadmap are important elements of a successful mobile collaboration and communications strategy. A brief description of essential features for a valuable and sustainable secure mobile communication solution is provided below.

Product Capabilities

Both Urgent Messaging and Secure Messaging are important for effective smartphone-based communication in hospitals. Support for rich media and voice calls is also critical. At the very minimum, the solution should be able to support the following modes of communication:

- Person-to-person secure text messaging, voice calling, and clinical content sharing;
- Machine-to-person secure text messaging and clinical content sharing; and
- Patient-provider secure text messaging, voice calling, and clinical content sharing.

2 The Emergency Care Research Institute (ECRI), an independent, non-profit organization focused on researching best practices in patient care.

Other important product capabilities include:

- **Integration with hospital IT systems:** Valuable integration includes EHR, nurse call systems, patient monitoring systems, bed management solutions, radiology and laboratory result solutions, etc. Effective integrations with identity and access management systems are also important.

- **Send and receive messages from other connected devices:** Solutions should be multi-device and should support real-time data synchronization. They should enable communication and collaboration across a variety of devices (and applications) used within the clinical environment, including other smartphones and tablets, connected wearables, email, PCs, phone systems, and pagers.

- **Support multiple directories on a single device:** Healthcare workers can work in multiple facilities and need the ability to access and communicate using up-to-date directories that cover the facilities and groups they work from each day. Also, the system should enable them to connect with their places of work and extended care team through a single application (or a single device), rather than requiring them to carry multiple devices.

- **Role-based and activity-based calling:** In critical-care environments, communication scenarios and personnel vary on a daily basis. Healthcare workers often think of the "role" of the person they are trying to call versus the person themselves. The communications solution should enable staff members to easily find and communicate with their colleagues inside or outside the hospital across the entire continuum.

- **Cellular, as well as Wi-Fi communication capabilities:** Having reliable communication is critical. The communication system should be able to let care team members communicate with each other from smartphones over both cellular and Wi-Fi networks to enable collaboration wherever the care team member happens to be.

- **Alarms communications and context:** Reducing alarm fatigue and providing proper context when a communication event is initiated are important. The care team member should be able to get the "context" of the alarm, which can be enabled by integrating the secure communication platform with the EHR, location systems, scheduling systems, and other hospital IT platforms.

- **Accommodate the diverse endpoint needs of hospitals:** Hospitals are not homogenous environments. For example, the needs of a nurse versus the needs of a transport tech are very different. Secure communication solutions should support a diverse range of devices and communication methods, and staff members should be able to pick the most appropriate device and method according to their unique requirements and context of use. Communication should be interoperable between device types, data transmission types, and locations. Taking a "device-of-choice" view is critical for long-term success. Case in point, Vocera's communication system provides an integrated suite of communication solutions that work on smartphones, tablets, and hands-free "badges." This flexibility provides users with the option to select the most appropriate and effective device and communication method for the situation. Nurses are typically delivering patient care when they receive calls so they prefer a hands-free voice-controlled "badge," while doctors typically prefer secure text messaging through a smartphone. A key decision point for clinical and administrative leaders is to select a communication system that enables choice of device to provide seamless collaboration between care team members inside and outside a facility.

Ease of Deployment

- Turnkey implementation, product extensibility, modularity, and a strategic roadmap are essential for long-term success. As a healthcare organization and its requirements change and expand, the communication system for voice and text messaging should have the ability to scale, deeply integrate, and evolve.

- A detailed assessment of existing and planned hospital IT infrastructure can help ensure proper, trouble-free deployment. Larger organizations may request deployments on their private cloud. Such opportunities should not be ignored and solution providers should be flexible with their deployment models.

User Experience and Customer Support

- **Mobile device efficiency:** An application on the mobile device should not consume too many device resources.

- **The solution should be simple to use:** Users should be able to easily download the secure mobile communication application without the need to go through complicated product configuration steps.

- **Ease of management:** Healthcare IT personnel should be able to easily manage the secure mobile communication solution. Proper training (training materials, knowledge portals, and self-serve portals) should be provided to all customers.

- **High availability:** Solution providers should be able to commit to higher levels of availability in their service-level agreements (SLAs) as well.

- **Return on investment (ROI):** Solution providers should help their customers understand the ROI for their investments in secure mobile communication solutions. It is important to provide customers with the right tools to help them measure the performance (and benefits) of secure mobile communication solutions that have been deployed.

RECOMMENDATIONS FOR HEALTHCARE FACILITIES

- Frost & Sullivan firmly believes hospitals should evaluate, on a priority basis, how enterprise-grade secure mobile communication solutions can help reduce communication and collaboration breakdowns within their facility and across multiple sites. Organizations should, at the very minimum, deploy a pilot program to evaluate how to leverage the potential of smartphones in their environments. Simple point solution and "freemium" applications may offer extended trials of their solutions, yet in the long run, may increase complexity due to the need to use multiple applications or limited extensibility across sites. Note that "freemium" trials may not demonstrate the value of a system that is truly integrated into a hospital's IT infrastructure or extendibility across multiple sites as these solutions tend to be pure applications and are not enterprise-grade communication tools.

- Hospitals should take a long-term view of their mobility strategies. They cannot continue to depend on older technologies simply because they are well-entrenched into their environments. Support for older-generation products, such as pagers, can and will end. The current set of available smartphone-based solutions is extremely easy to implement and guaranteed to be around for a long time.

- Apart from supporting corporate-liable devices, healthcare facilities should also consider supporting BYOD and shared devices, or at a very minimum develop a BYOD policy. This approach can help hospitals lower the cost of deploying secure mobile communication solutions. However, there is no "free lunch" with BYOD. A true ROI measurement must consider improved staff productivity, increased revenues, impact on patient and staff satisfaction, potential for staff retention, and direct and indirect cost of BYOD implementation and management.

- As hospitals look to embrace a mobility strategy, they need to ensure the chosen solutions can deliver on various security and compliance-related requirements, particularly related to data encryption and remote data wipe, which includes the possible need to ensure that sensitive data is automatically made unavailable from mobile devices after they have been disconnected from the network.

- Hospitals are expected to see increased requests for device configuration and support, and should ensure that users are able to use the existing helpdesk systems that support other connected endpoints (such as PCs) and enterprise apps. The need for an exceptional customer experience also makes it critical to work with vendors with proven customer support capabilities.

THE LAST WORD

By eliminating time spent on less-productive activities, and by helping organizations adhere to industry best practices, enterprise-grade, secure smartphone solutions can help hospitals deliver better patient care when deployed as part of a broader enterprise strategy that supports communication and collaboration across multiple devices like smartphones, hands-free badges, tablets and desktop computers. A critical evaluation of the available options is important to ensure fool-proof deployments and for achieving the best return on investment in such solutions. Many leading secure mobile communication solution providers can implement pilot programs that can help hospitals evaluate the benefits of secure mobile communication solutions. Hospitals should look to partner with a trusted communications system provider that offers a comprehensive portfolio of best-in-class solutions and a proven track record. Given the new market landscape, now is the time for non-users to run the numbers and consider next-generation secure mobile communication solutions.

LEGAL DISCLAIMER

Quantitative market information is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan is not responsible for incorrect information supplied to us by manufacturers or users.

Our research services are limited publications containing valuable market information provided to a select group of customers. Our customers acknowledge, when ordering, subscribing or downloading, that Frost & Sullivan research services are for customers' internal use and not for general publication or disclosure to third parties.

No part of this research service may be given, lent, resold, or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the permission of the publisher.

Auckland
Bahrain
Bangkok
Beijing
Bengaluru
Buenos Aires
Cape Town
Chennai
Colombo
Delhi/NCR
Detroit
Dubai
Frankfurt
Houston
Iskander Malaysia/Johor Bahru
Istanbul
Jakarta
Kolkata
Kuala Lumpur
London
Manhattan
Miami
Milan
Mumbai
Moscow
Oxford
Paris
Pune
Rockville Centre
San Antonio
São Paulo
Seoul
Shanghai
Shenzhen
Silicon Valley
Singapore
Sophia Antipolis
Sydney
Taipei
Tel Aviv
Tokyo
Toronto
Warsaw

Silicon Valley
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10,
Suite 400
San Antonio, TX 78229
Tel 210.348.1000
Fax 210.348.1003

London
4 Grosvenor Gardens
London SWIW 0DH
Tel +44 (0)20 7343 8383
Fax +44 (0)20 7730 3343

877.GoFrost
myfrost@frost.com
www.frost.com

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?

For information regarding permission, write:
Frost & Sullivan
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041