WHITE PAPER

Amcom SOFTWARE

The Role of Mobility Strategies in Healthcare: 2013 Survey Results

Introduction: Mobile Healthcare Communications

Over the past two decades the landscape of healthcare communications has been changing rapidly. While whiteboards and patient binders are still in use, much of the information previously conveyed via paper has gone electronic - orders, test results, diagnoses, consultation notes, etc. Patient scans can be reviewed by radiologists a world away from the ordering physician. Providers can enter treatments into the computer while examining a patient at the bedside, and the order can be immediately received by the desired contact. This shift to electronically stored information and instant forms of communication increases the speed of patient diagnosis and efficiency of treatment, ultimately improving patient care and satisfaction.

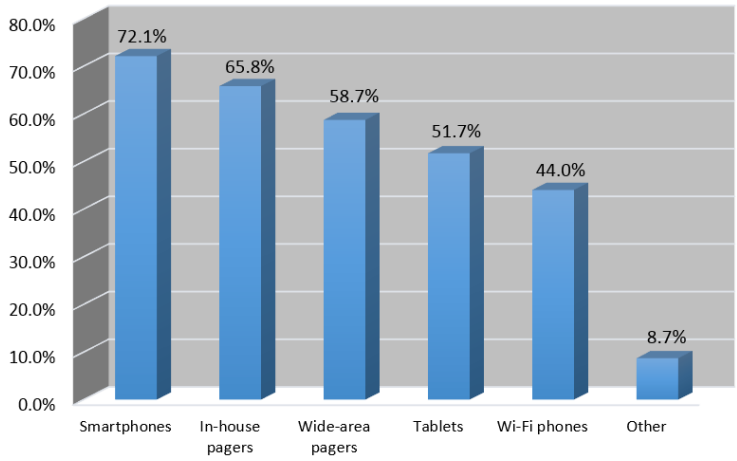

Figure 1. Which types of mobile devices does your organization support?

The method of electronic communication continues to evolve as smartphones, tablets and other mobile devices become the preferred tools for providers. With this new technology comes a lot of new questions, too. What types of devices do hospitals allow and support? Can providers use their personal devices or must they use facility-issued ones? Are the mobile communications secure? Are there documented policies and procedures governing mobile device usage?

2013 Mobility Strategy Survey

Since 2010, Amcom Software has been deploying an annual survey to gauge mobile communication trends in the healthcare space and track year-over-year changes. In June 2013, Amcom once again implemented this survey, which was completed by more than 550 healthcare professionals. It allows us to better understand how healthcare facilities are addressing these communication questions and to see how far along hospitals are in devising their strategies. Survey participants were from hospitals of all sizes across the globe and included leadership in the departments of clinical, IT, and telecommunications.

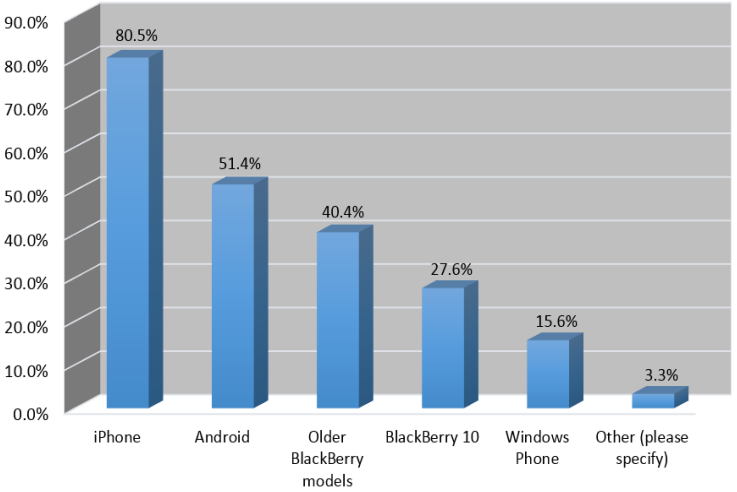

Figure 2. If you selected "Smartphones," what type of smartphones does your organization support?

The results of this year's Healthcare Mobility Strategy survey found today's hospitals are supporting a wide range of communication devices (Figure 1). While smartphones and pagers are the most commonly supported devices, tablets, Wi-Fi phones, regular cell phones and laptops are also included in the mix. Since last year's Mobility Strategy Survey, the devices with the largest increase in support were

smartphones (12.7% increase), wide-area pagers (5.9% increase), and tablets (3.1% increase). Amcom broke this question down further to determine the specific types of smartphones people are using to communicate. iPhone® smartphones took the lead with more than 80% of organizations providing support, followed by Android® smartphones at 51.4% (Figure 2).

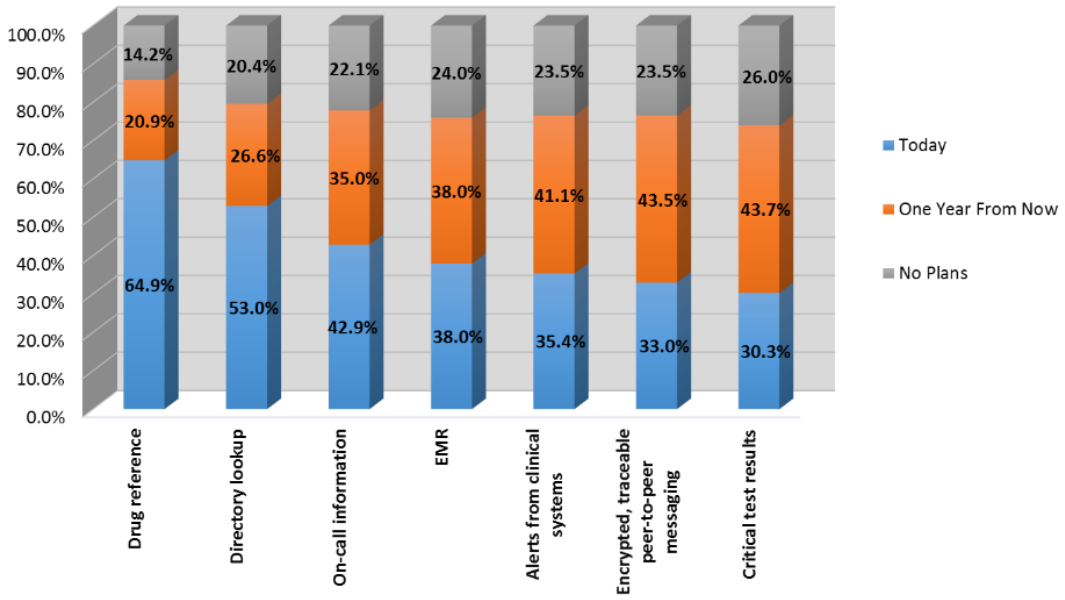

Figure 3. What types of information do smartphone users have access to today and will have one year from now?

As the number of smartphones being supported increases, there is also an increase in the amount and type of information clinicians can access from their phones. The top areas of information currently accessed from smartphones are drug references, directory lookup, and on-call information (Figure 3). Respondents noted that one year from now they expect to see the greatest increase in access to critical test results (43.7%), encrypted peer-to-peer messaging (43.5%), and alerts from clinical systems (41.1%). Since last year's survey, access to encrypted peer-to-peer messaging on smartphones saw the largest increase with 11%.

The next question Amcom asked was if the organization had a documented mobility strategy in place. 44.4% of the healthcare facilities surveyed have a written policy, which is a 10% increase over last year. Of the facilities that do *not* have a written policy, 30.2% are currently working on one, and 20.3% have a verbal policy. Some of the reasons respondents mentioned for not having a documented strategy are budget constraints, that it is not a high priority, a lack of awareness, or that there is no one to take the lead in development (Figure 4). Thirty-five percent of respondents said there are no plans to implement a mobility strategy in their organization.

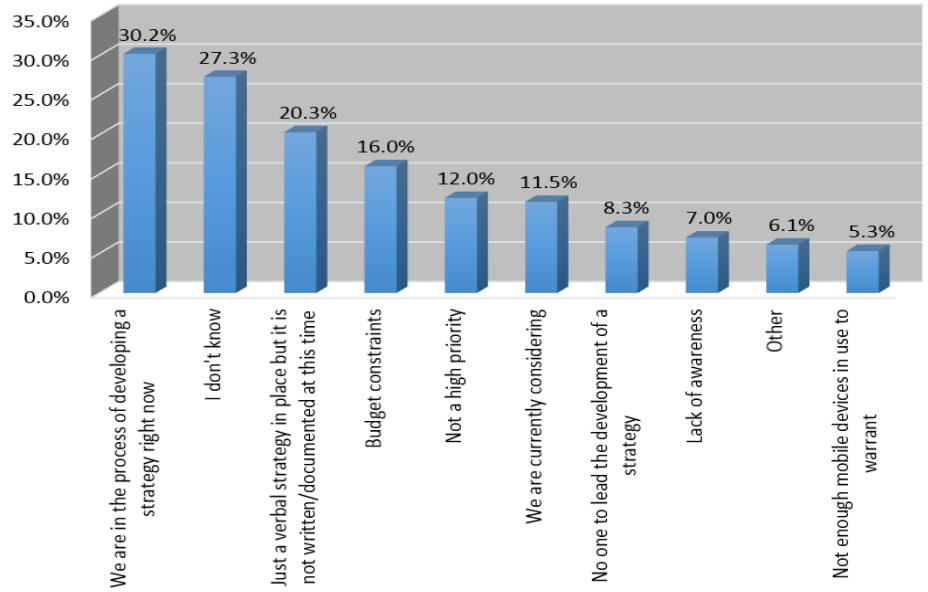

Figure 4. Why is there no mobility strategy in place at your hospital? (For individuals who answered "no" to having a mobility strategy.)

Those surveyed were also asked what topics were important when developing a mobility strategy. The top three identified were 1) security 2) budget, and 3) ability of mobile devices to run on the hospital Wi-Fi network (Figure 5). The rest of this paper will explore these topic and solution ideas for each category.

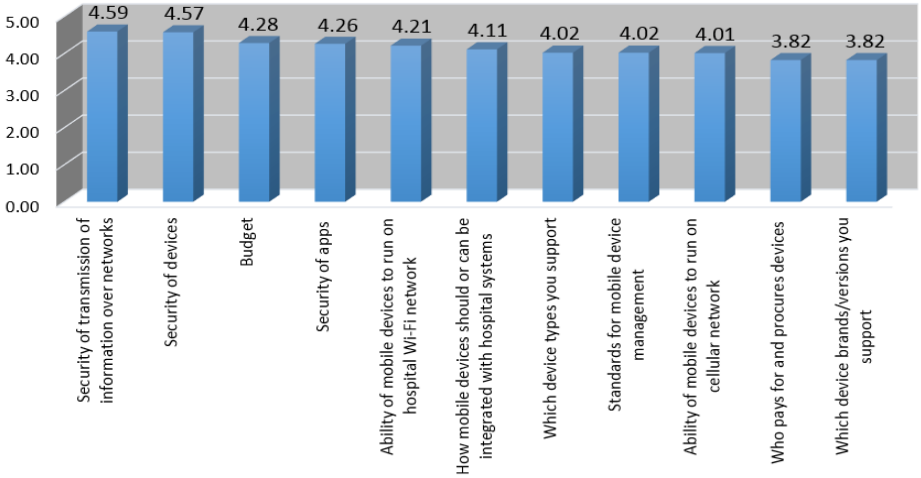

Figure 5. On a scale from 1-5, how important are the following areas when and if you develop a mobility strategy?

Device and Information Security

History of HIPAA, HITECH and the Security Rule

Mobile device security is an incredibly important topic. Specific concerns in this area include the security of information contained on a lost or stolen device, the security of information transferred over wireless networks, and the security of applications running on the devices. While these topics are certainly challenging, the good news is there are viable solutions to address each of these points, as well as

improve overall communication processes. Before looking at the solutions, however, let's examine the history and current state of data privacy rules.

Security considerations mandated by the Health Information Portability and Accessibility Act of 1996 (HIPAA) are largely imposed by the Security Rule amendment published February 20, 2003. The Security Rule (45 CFR Parts 160, 162 and 164), states that "Covered entities must…ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains or transmits…[and] protect against any reasonably anticipated threats or hazards to the security or integrity of such information."[1] Further, section § 164.308 (a)(1)(i) says "*Standard: Security management process.* Implement policies and procedures to prevent, detect, contain and correct security violations."

The first compliance mandates for HIPAA took effect in 2003, and over the next four years approximately 8,000 cases were closed with no significant penalties.[2] Initially appearing to merely be a helpful entity offering organizations greater awareness of the rules surrounding protected health information, the U.S. Department of Health and Human Services (HHS) began imposing significant financial consequences with case settlements in 2009. [3,4]

In the mobility strategy survey, Amcom asked, "Are you aware of the Joint Commission guidelines on texting patient orders?" - Only 59.2% of respondents said "yes."

Also in 2009, the American Recovery and Reinvestment Act (ARRA) was passed by Congress. Primarily intended as a stimulus bill, ARRA included the Health Information Technology for Economic and Clinical Health Act (HITECH), which not only broadened HIPAA's scope, but it also upped the ante by increasing fine limits and providing a big incentive for investigators to examine reported violations. With HITECH in place, fines are paid to the HHS Office of Civil Rights (OCR) Enforcement[4] – thus the investigators now pay themselves.

Violation by Mobile Device

Since late 2011, multiple HIPAA violations resulting in fines have had to do specifically with the security of mobile devices: a USB drive was stolen from an Alaskan HHS employee's vehicle ($1.7 million)[5], 57

[1] Federal Register Vol. 68 No. 34, "Rules and Regulations." § 164.306 (a)(1) & (a)(2). Feb 2003. https://www.cms.gov/Regulations-and-Guidance/Regulations-and-Policies/QuarterlyProviderUpdates/Downloads/cms0049f.pdf

[2] Korzeniowski, Paul. "HIPAA: Clean bill of health, or dying a slow death?" SearchFinancialSecurity.com. 18 Jan. 2008. Web. 7 Aug. 2012. http://searchfinancialsecurity.techtarget.com/news/1294167/HIPAA-Clean-bill-of-health-or-dying-a-slow-death

[3] Federal Trade Commission. "CVS Caremark Settles FTC Charges: Failed to Protect Medical and Financial Privacy of Customers and Employees; CVS Pharmacy Also Pays $2.25 Million to Settle Allegations of HIPAA Violations." 18 Feb. 2009. Web. 7 Aug. 2012. http://ftc.gov/opa/2009/02/cvs.shtm

[4] Proofpoint, Inc. "HIPAA Update: Keeping Compliant with the Latest Healthcare Email Security Regulations." 2012. Web. 7 Aug. 2012. http://www.proofpoint.com/id/PPC-HIPAA-email-security-whitepaper-2012/index.php?utm_source=adwords&utm_medium=ppc&utm_term=hipaaemailcompliance&utm_content=hipaawp&utm_campaign=hipaaemailcompliance&gclid=CPmi7oSsurECFSMCQAodQEAAEw

unencrypted hard drives were stolen from a storage facility (Blue Cross Blue Shield of Tennessee, $1.5 million)[6], and a Resolution Agreement for an Arizona physician group made particular mention of the need to secure ePHI (electronic protected health information) contained in text messages.[7] According to the Joint Commission's statement in 2011, texting patient orders is not acceptable.[8]

Texting security requirements, as well as multiple reported incidents of unencrypted laptop thefts[9,10,11] prompt questions about mobile device security. Luckily, all of these security breaches are preventable. Going a step further, the right investment in communications technology can not only bring devices in line with security compliance regulations, but it can also improve communication workflows, increase staff satisfaction, and promote better patient outcomes.

Mitigating the Risks

63% of survey respondents expressed concern specifically around PHI security on smartphones. The survey also revealed smartphone use is currently split between hospital issued and personal devices (nearly 46%/54%), and mobile devices are used primarily to increase efficiency and facilitate communication among providers (Figure 6). So what are the risks?

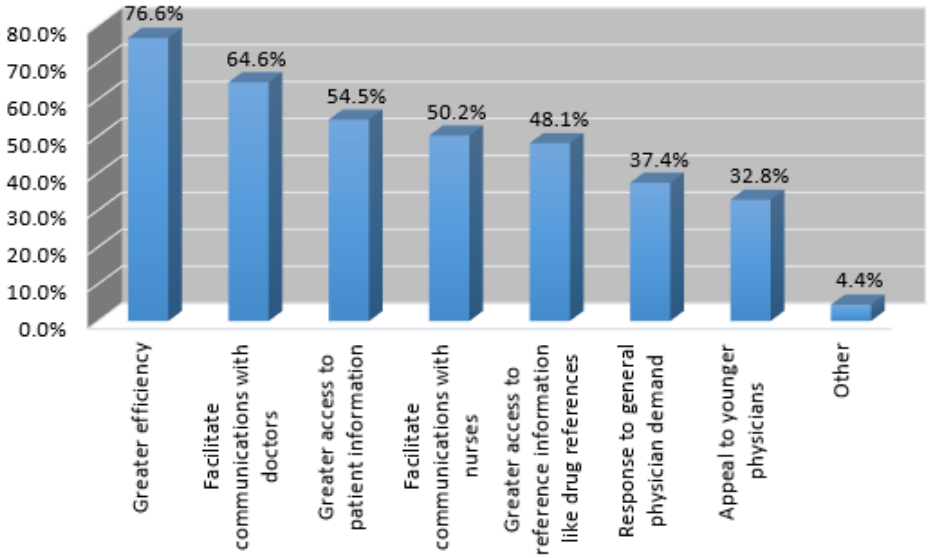

Figure 6. What are the main drivers of using smartphones and other mobile devices?

[5] U.S. Department of Health and Human Services. "Alaska settles HIPAA security case for $1,700,000." 26 June, 2012. Web. 7 Aug. 2012. http://www.hhs.gov/news/press/2012pres/06/20120626a.html
[6] U.S. Department of Health and Human Services. "HHS settles HIPAA case with BCBST for $.5 million." 13 Mar. 2012. Web. 7 Aug. 2012. http://www.hhs.gov/news/press/2012pres/03/20120313a.html
[7] U.S. Department of Health and Human Services. "HHS settles case with Phoenix Cardiac Surgery for lack of HIPAA safeguards." 17 Apr. 2012. Web. 7 Aug. 2012. http://www.hhs.gov/news/press/2012pres/04/20120417a.html
[8] The Joint Commission. "Standards FAQ Details." 10 Nov. 2011. Web. 7 Aug. 2012. http://www.jointcommission.org/standards_information/jcfaqdetails.aspx?StandardsFaqId=401&ProgramId=1
[9] Berger, Jerry. "BIDMC Notifying Patients of Potential Computer Data Breach." 23 July, 2012. Web. 7 Aug. 2012. http://www.bidmc.org/News/AroundBIDMC/2012/July/LaptopBreach.aspx
[10] Stewart, Rebecca. "Hartford Hospital and VNA Healthcare Notify Patients of Computer Theft."30 July, 2012. Press Release. 7 Aug. 2012. http://www.harthosp.org/Portals/1/Images/6/PR-VNA-Data-Incident.pdf
[11] Lathan, Kris. "Statement Regarding Hospice Burglary and Patient Information Breach." 25 July, 2012. Web. 7 Aug. 2012. http://www.nmh.org/nm/home-hospice-burglary-noticed

As illustrated by some of the HIPAA settlements mentioned above, there are several risk factors to consider during the development of a mobile security policy, for both bring-your-own-device (BYOD) programs and company-issued equipment.

- Are the devices password protected?
- Are password policies enforced?
- Is remote data wipe enabled?
- Is mobile security software installed to protect against viruses or malware?
- Is the wireless network secure?
- Is the data sent with encryption?
- Is a password required to retrieve data containing ePHI?
- Are mobile apps safe and secure?

When HIPAA was first enacted, smartphones were not widely used. (Bell South released Simon in 1994; Research in Motion (RIM) did not put out the BlackBerry® until 1999.) The Security Rule predates both the iPhone® and iPad®, released by Apple in June 2007 and April 2010, respectively. Despite their newness, however, the use of these types of devices for the communication of protected health information falls within the scope of the Security Rule.

The answers to these questions include a combination of policy solutions and security features that can be provided by both hardware and communication software. Solutions are currently available in the marketplace that provide device security and message encryption with patient monitoring, peer consultations, delivery of test results, and more.

In May 2012, the Department of Homeland Security released a National Cyber Security and Communications Integration Center bulletin about healthcare and the public sector.[12] The bulletin makes multiple recommendations to protect against imminent cyber security threats, including "establishing strict policies for the connection of any networked devices, particularly wireless devices, to [the] Health Information Network (HIN), including: laptops, tablets, USB devices, PDAs, smartphones, etc., such that no access to networked resources is provided to unsecured and/or unrecognized devices." To protect patient information, Homeland Security also advises securing communications channels with encryption, requiring user authentication at both ends, and enforcing password policies.

In addition to having documented policies surrounding passwords and device access to wireless networks, health organizations will want all mobile communication devices used for care delivery and ePHI data transmission at their facility to operate with specific features such as remote data wipe and updated virus protection. Understanding how hospital staff uses their mobile devices to communicate with one another will help in the selection of appropriate solutions to support and even enhance the communication workflow.

[12] U.S. Department of Homeland Security. "Attack Surface: Healthcare and Public Health Sector." 4 May, 2012. Bulletin. 7 Aug, 2012. http://info.publicintelligence.net/NCCIC-MedicalDevices.pdf

Another way organizations work to maintain secure communications is through the use of a Mobile Device Management (MDM) solution. A MDM solution allows organizations to securely enroll devices in an enterprise environment, configure and update settings, monitor compliance with corporate policies, and remotely wipe or lock managed devices. Only 21.3% of survey respondents said they are currently using a Mobile Device Management solution in their organization, but 30.8% of respondents are currently evaluating implementing one (Figure 7). Of those using an MDM solution in their organization, 84.8% are using them on corporate-owned devices and 56.2% on individual-owned devices. Some of the most important features organizations look for in an MDM solution are device encryption, enforcement of device password, and remote wipe/lock.

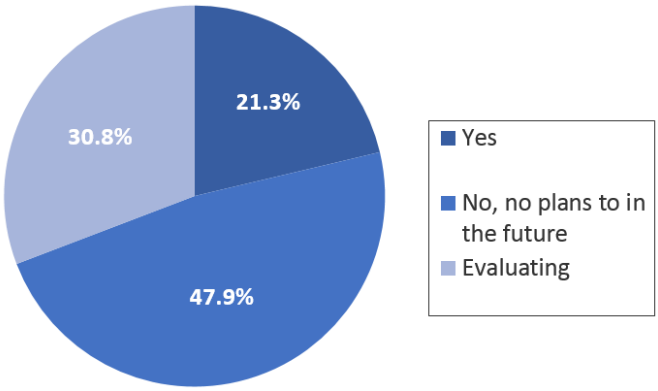

Figure 7. Are you using a Mobile Device Management (MDM) solution in your organization?

Budget vs. Cost

Budget was identified as survey respondents' second most important concern relating to development of a mobility strategy. Budget was also cited as an issue preventing 16% of hospitals without a documented mobility strategy from developing one. Designing, implementing and integrating a mobile device strategy includes employee time to initiate, plan and develop; vendor costs for hardware and software; maintenance; and device-related user costs. A good mobility plan can, however, improve provider efficiency, provide cost savings to facilities, increase staff satisfaction, and ultimately improve patient care.

In healthcare, the idea of efficiency doesn't necessarily evoke thoughts of better care. Most patients probably want to spend more time with their providers to really understand their health issues and treatment options. Improving mobile communication efficiency will actually allow providers to spend more time at the bedside by reducing time spent managing communications at a desk or nursing station. Mobile communications platforms can also support immediate provider-to-provider consultations, allowing faster decision-making. Overall, improved communication efficiency will allow providers to do more with less.

One of the major drivers of dollar savings with a well-implemented mobility plan is the use of communications technologies that provide traceable messaging. Systems that track when messages are created, sent, received and acknowledged provide an audit trail of traceable proof that communications were transmitted and received. If there is ever litigation against the hospital or its providers, this audit trail serves as documented evidence of the care process. Providing this type of closed-loop communication can reduce physician malpractice insurance costs by an estimated 15% annually.[13]

[13] Metric derived from collaboration with SaferMD http://www.safermd.com/.

Tracking also ensures if critical messages are not acknowledged quickly they can be escalated to another provider. This keeps patient care on track and can improve the outcome.

Savings can be further enhanced in a BYOD setting where the cost of the devices and plans is borne in part by the employees, who are often happier to use their own, familiar device, and can upgrade when they choose, not when a budget permits.

BYOD

Bring Your Own Device approaches were supported by 56.5% of hospitals surveyed. When further asked if the organization allowed/required remote wipe capabilities of the BYOD device in case of loss or theft, 29.9% said "no."

Communication systems that provide messaging capabilities through both Wi-Fi and cellular networks can reduce cellular plan costs by using Wi-Fi inside the facility, decreasing data usage. This is an important feature for hospitals that have dead zones where cellular service is very weak or unavailable, especially in imaging labs and operating suites that may have been built on the lowest levels or in the heart of a facility.

Addressing the previous discussion about security, communication software platforms are available that mitigate many potentially costly security risks of hospital-provided and BYOD devices. This is possible by sending all messages in an encrypted format, delivering them to segregated inboxes on the devices that require passwords (keeping personal information separate from professional and securing potentially sensitive information), and providing remote-wipe capabilities in the event a device (such as a smartphone) is lost or stolen.

When deciding whether to pursue a full mobility strategy where budget is a major consideration, organizations need to incorporate the positive outcomes from implementing a comprehensive plan. This includes efficiencies gained, improved patient outcomes, insurance premium savings, increased staff satisfaction, equipment cost savings, and enhanced HIPAA and HITECH compliance. All are important to consider as part of the overall cost model.

"The cost of dealing with a security breach is greater than the cost to have secured the personal device." [4]

- John Halamka, M.D., Professor of Medicine at Harvard Medical School and CIO at Beth Israel Deaconess Medical Center, at the mHealth World Congress, July 2012

Integration & Planning

The third most important mobility strategy topic hospitals identified is how to integrate all of the systems and sources of data to deliver the right message to the right person on the right device at the right time. Even without a mobility policy framework, coordination of information is a central issue for health facilities as they bring islands of information together for efficient and effective care. Patient updates, diagnostic test results, consult requests, code alerts, patient monitoring devices – all of these sources of information need to be channeled to the correct individuals on time, whether they are on site or on call.

[14] Durben Hirsch, Marla. "Security of mobile devices a continuing concern." 27 July, 2012. FierceMobileHealthcare. Web. 7 Aug, 2012. http://www.fiercemobilehealthcare.com/story/security-mobile-devices-continuing-concern/2012-07-27?utm_medium=nl&utm_source=internal#ixzz22DubbM9E

One way to begin bringing communications together is through a complete web directory. A web-based staff directory can save time on multiple fronts and significantly reduce internal calls to the operators. Having the directory available to staff on their mobile devices also provides faster peer consultations and requests for assistance.

Using a web directory system, facilities can add staffing rotations and on-call schedules, as well as the on-call staff member's preferred method of communication and/or device type at different hours (smartphone, home phone, e-mail, text, pager, etc.), further decreasing the time it takes to connect with the right person in time-critical situations.

With staff availability and contact preferences consolidated into a single directory, systems integration becomes easier. Clinical alerting solutions or other software products, such as applications that allow communications to be handled based on physician preferences, can be programmed with logic to locate the right person on the right device. Whether searching for a specific person or a position title (e.g., the on-call cardiologist), employees can easily and quickly dispatch a message to the correct individual on their preferred device, with escalation protocols built in if there is no response. Having a mobile platform in place also enables hospitals to deliver patients' critical test results from the Lab, Radiology, and other departments to mobile devices in a fast and secure manner.

Conclusion: The Need for a Mobile Plan

Mobile communications are convenient, efficient and familiar, and mobile device usage in healthcare is continuing to increase as more caregivers rely upon them for instant notifications. The challenge for everyone, from large hospitals to small private practices, is integrating all data and information sources with multiple devices while ensuring the security of ePHI that is carried on and transmitted by these highly portable smartphones, tablets, etc. Luckily, making the right investments in mobile communications technology can save money, increase staff satisfaction, and improve patient care.

Documenting a mobility strategy will prompt discussion around overall hospital communications. Assessing and prioritizing the communication needs for the entire organization will catalyze an examination of the products, services and processes that increase efficiency, save time, and promote patient safety across the organization. Ultimately, the use and integration of mobile devices will benefit patients by reducing administrative time spent managing communications, allowing providers to spend more time directly administering and coordinating care. Designing and implementing a comprehensive mobility strategy is a critical step in securing patient privacy and enhancing patient safety in the age of portability.

About Amcom Software

Amcom Software, a subsidiary of USA Mobility, Inc. (NASDAQ: USMO), connects people to each other and to the data they need. This helps organizations save lives with communications that are faster, more accurate, and more efficient. Thousands of organizations worldwide rely on Amcom solutions for critical smartphone communications, contact center optimization, emergency management, and clinical workflow improvement. The company's products are used by leading organizations in healthcare, hospitality, education, business, and government. By continually developing its industry-leading technologies, Amcom Software has steadily grown and solidified its market leadership.

Amcom SOFTWARE

www.amcomsoftware.com