



Case Study:
**MAKING HEALTHCARE
MOBILE**

**A Guide for Mobile-Enabling Electronic Health Record,
Chronic Care Management & Other Healthcare IT Systems**

Written by: mPulse



PUBLISHED BY

mPulse Mobile Inc.



© 2015 mPulse Mobile — All rights reserved.

www.mPulseMobile.com

16530 Ventura Blvd. Suite 502
Encino CA, 91436

Telephone (805) 200-4848

Copyright © 2015

No part of the contents of this publication may be reproduced or transmitted in any form or by any means without the written permission of mPulseMobile Inc.

mPulse Mobile is a registered trademark of mPulse Inc.
All other trademarks are the property of their respective owners.



OVERVIEW

This guide is intended for an audience composed of businesses that offer web-based solutions to the Healthcare Industry. Examples include systems for electronic medical health records, practice management, disease/chronic care management, medication adherence or software and online services supporting health plans, providers, and pharmacies.

You may be considering adding a mobile communication element to your products or services. In this paper, we will give you information to help you evaluate and plan for using secure “inapp” messaging and SMS as part of your communication systems and provide some insight into the process and challenges.

Innovate or die – it’s no revelation that mobile healthcare applications are one of the hottest topics of conversation in healthcare. The buzz and investment in the move to mobile-enabled data access and communications has accelerated at an amazing pace since early 2010.

Mobile development in healthcare is being driven by innovation in the tech sector, cost saving initiatives by providers and payers, and overwhelming demand by consumers. Benefits are farreaching and centered on solving problems:

- Healthcare Providers – want to use mobile to contain costs and improve the quality of care. The healthcare industry moves slowly and with good reason. Healthcare is a complex business.
- Healthcare Payer Organizations – see mobile as a way to control more of the services delivery pipeline as a way to build more direct and real-time involvement in member healthcare decisions. The concept of preventive care being a way to lower costs is also important to payer organizations.

In this guide, we will explore why mobile-enabling your healthcare systems products may make sense and provide insight into the challenges and solutions involved in harnessing the power of mobile communications.

CONTENTS

Overview	3
Why Mobile Makes Sense for Healthcare IT.....	5
Data Access	5
Communications	6
HIPAA/HITECH and Mobile	8
The Law(s)	8
What Does It Mean For Mobile	9
What You Should Know About Mobile Best Practices	11
Industry Rules – A Few Basics	11
Legal/Regulatory – Important Highlights	13
A Note on the Mobile Marketing Association	13
In-App Messaging	15
Opportunities	17
SMS Messaging	18
Acceptable Uses of SMS with PHI in Healthcare.....	19
Project Considerations	20
Proof of Concept (“POC”) and Pilot Projects	20
Proof of Concept	20
General Mobile Advice	21
SMS Specific Challenges	21
App Message Considerations	22
Pilot Projects	23
A Checklist for Conducting a Pilot	24
Pilot Program tips.....	25
During the Pilot.....	25
After the Pilot.....	26
Choosing a Mobile Partner	27



WHY MOBILE MAKES SENSE FOR HEALTHCARE IT

Using mobile technologies in healthcare is sometimes referred to as mHealth, and these applications cross a very broad spectrum of services, data sources, and channels. Because of smartphone and cellular data network progress, mobile device capabilities are becoming equal to and greater than that of desktop or even laptop computers.

Compare what can be accomplished with a small travel laptop to what can be done with a smartphone. Using an Android or Apple Smartphone you can access data, send/receive email, do routine word processing or editing, watch movies – some would argue you can do more with a smartphone than with a PC -- all in a package that's certainly more convenient and accessible than a laptop.

A large part of the mobile “revolution” is mobile devices taking over some of the work previously done by desktop and laptop computers. After all, a smartphone is simply a very small, portable computer that you take with you almost anywhere you go.

DATA ACCESS

While this paper will focus on using mobile technology to communicate, it's useful to reflect that mobile is already here for any data accessible via the web.

If you're in the healthcare IT industry, you know that patients and plan members having electronic access to their medical records is not the industry norm, it's an exception. Today, strong governmental requirements, along with good business practices, are pulling down some of the obstacles – at precisely the time when consumer use of mobile devices is eclipsing work done from a desk.

Consumers have a very high interest in communicating electronically with healthcare professionals. In a survey conducted by Capstrat, consumers were asked about the medium in which they'd like to communicate with their doctor and other health providers.

- Over 54% of consumers indicated they wanted advice online from nurses via email.
- Almost 53% said they wanted two way email communication with their doctor.
- Over 51% said they wanted online access to their medical records.

COMMUNICATIONS

Some of the most compelling benefits of mobile in the healthcare environment are focused on communicating with patients and members. Communications may be on a one-to-one basis between a healthcare professional and a patient or may reach out to groups with pertinent and timely information. And with mobile, communication can be two-way and interactive. Interactivity can be provided by logic in a healthcare system or between two, or even thousands, of people.

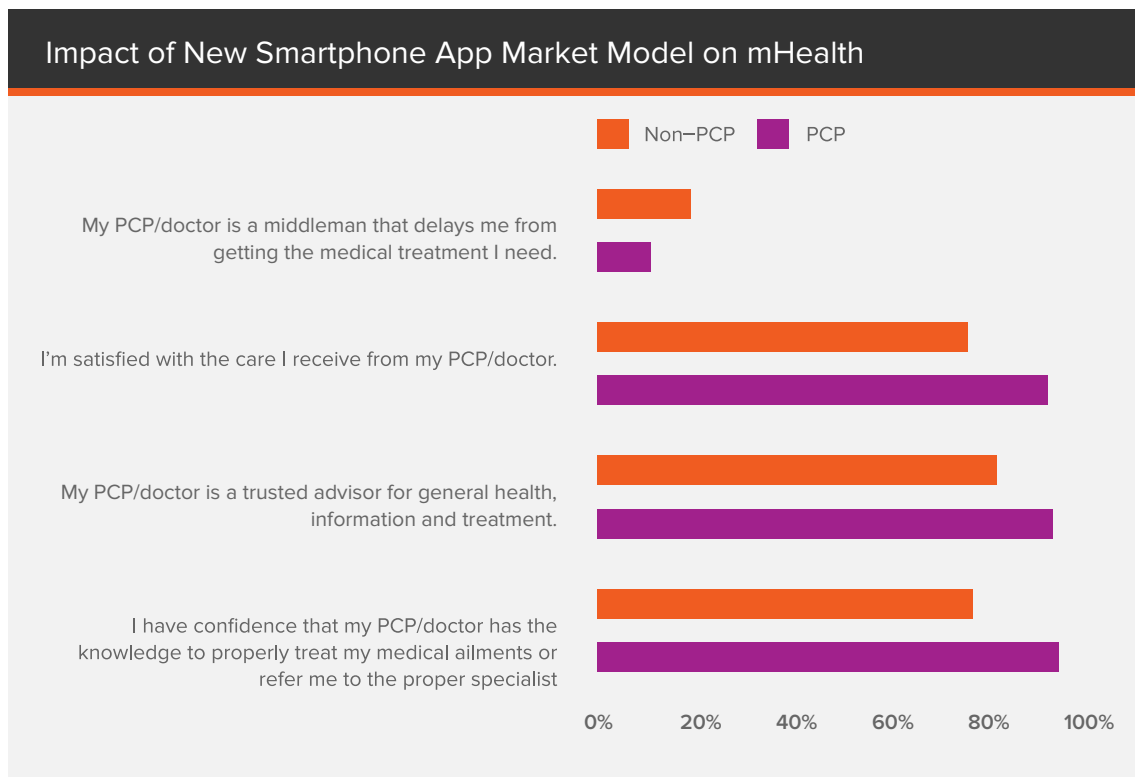


Consider the implications in terms of cost management to the healthcare organization and quality of life to the members when using mobile for:

- **Appointment Reminders** – Send automated reminders to decrease missed appointments.
- **Chronic Condition Management** – Send programmed message sequences to encourage adherence to a disease or condition management plan.
- **Payment and Member Account Communications** – Send message regarding accounting issues, late payments, changes to the health plan, or open enrollment solicitation.
- **Health Alerts** – Send a specific notification that needs to reach a user or group. E.g. “You’re overdue for a tetanus shot.”
- **Medication Adherence** – Send messages such as, “Time to take your Riboflavin pill. Please reply back ‘Yes’ when you’ve taken your medication.”
- **Status Collection** – Poll users regarding pain level, blood pressure, etc.

As you can imagine, the benefits to each of these programs could be huge for both the organization and its members. However, we have a hurdle to overcome in the healthcare industry: Sending Protected Health Information (PHI) via unsecured channels or storing PHI data in an unsecured manner is not allowed.

How best to overcome the obstacles? Mobile technologies provide opportunities to communicate securely with individuals or groups of plan members. Some of these methods will be discussed later in this paper.



Source: mPulse's [2015 mHealth Report](#)



HIPAA/HITECH AND MOBILE

The Law(s)

If you're reading this paper, it is likely you have at least some familiarity with privacy and electronic security requirements surrounding consumer health information as provided for by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The act was modified in 2003, in part by the addition of significant electronic security requirements.

HIPAA was originally created to make sure US healthcare patients would have access to their medical records. Access must be in an electronic format. HIPAA also contains a "Privacy Rule", which requires that consumer medical information categorized as PHI not be disclosed to anyone other than the person to whom it pertains or another person who has the legal right to view the information.

Since HIPAA, other federal and state legislation has been enacted that spells out requirements for the handling of PHI. The laws also support regulations developed and enforced by government agencies.

For example, in 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted as part of the American Recovery and Reinvestment Act of 2009. HITECH introduced several key amplifications to HIPAA including:

- Enforcement provisions and penalties for non-compliance.
- The concept of business associates: Vendors and contractors connected to the healthcare entity in certain ways.
- Notification of electronic security or data breach events.
- Requirement to provide electronic versions of healthcare information upon request by entitled consumers.

Other regulatory and agency-required rules exist, including the Department of Health and Human Service's security and privacy polices, Medicare/Medicaid rules for payers/providers serving their members. In addition, almost every state in the US has laws concerning privacy and disclosure of PHI.

WHAT DOES IT MEAN FOR MOBILE

The bottom line is that, unfortunately for all stakeholders, the application of the law to mobile transmission of healthcare related information is not clear. The types of data that can be electronically transmitted or received, the media allowed when transferring different types of data, and the method of transmission that is secure enough are not always clearly defined in any of the legislation or guidelines.

If fact, there remains enough ambiguity that mobile communication has been an area of careful interpretation for many in the healthcare industry, while others have stalled or not even begun to explore the potential.

Here are some examples:

- **Can I leave PHI in a message on a cell phone voice mail?**
 - Many healthcare companies are doing this today.
- **Can I send an unencrypted email to someone with their own PHI?**
 - Again, many organizations covered by HIPAA are doing this today.
- **Can I send an SMS message containing PHI to a member's cell phone?**
 - PHI is being sent between healthcare professionals and their patients daily, with or without any oversight approval.

Working with healthcare organizations using mobile technologies has been a primary focus for mPulse since 2007. In that time, we've seen the interpretation of how to communicate PHI data evolve. As consumer acceptance of the technology has grown wildly, healthcare organizations have been forced to confront the ambiguity and not surprisingly a wide variety of interpretations exist.

Each healthcare organization needs to make its own evaluation, and results may vary. We met a major healthcare provider that for almost a year chose to interpret

guidelines to mean that the act of sending any SMS to an identifiable cell number connects that cell phone owner to the healthcare provider – which in their initial opinion would constitute a disclosure of PHI. This read on the law was applied to any message – even if the message contained no data whatsoever. That particular organization has since revised its interpretation and is currently using SMS.





WHAT YOU SHOULD KNOW ABOUT BEST PRACTICES

Over the last several years, consumers have become much more accepting of mass SMS communications that are relevant. One reason is that the SMS communications channel has been protected from abuse by cell phone service carriers such as AT&T and Verizon. While there have been some cases of “spam” SMS messages, the industry is in a much stronger position to protect consumers against unsolicited messages. Compared to email, or even junk printed material, SMS enjoys a confidence from consumers that support it. Therefore, SMS continues to be a powerful medium.



If fact, most incidents of unsolicited SMS messages from legitimate businesses in the US are caused by a lack of understanding of the rules and best practices for delivering text communications. The relationship between consumers and their healthcare providers is among the most trusted in our society. It is critical that we

protect that relationship by understanding consumer expectations involving SMS and promoting compliance with rules and regulations that keep the channel open between consumers and their trusted healthcare providers and payers.

The consequences of purposefully – and sometimes accidentally - breaking the rules can be significant. In serious cases the right to send bulk SMS messages can be revoked by one or even all carriers. Even simple violations can sometimes trigger an audit from carriers, responding to which is time consuming and can be accompanied

by a service interruption. The Cellular Telecommunications Industry Association (CTIA), an independent, non-profit organization representing the international wireless industry, conducts some 20,000 audits per month to identify non-compliant programs and identify abuse to carriers.

There are many excellent guides to mobile best practices including mPulse's "[Digital Best Practices for Geniuses](#)." While the purpose of this document is not to provide a primer of mobile best practices, the basics of being a good mobile sender are outlined below.

INDUSTRY RULES – A FEW BASICS

- Rules apply to ALL senders of mobile communications. Often, healthcare providers or other businesses believe that a “special” relationship with the message recipient nullifies the rule established by the industry. This is an unfortunate misinterpretation that has led to extraordinary costs and downtime in several cases recently in which sending permissions have been revoked by carriers.
- Formal opt-in is required for ongoing SMS communications with a consumer. Similar to opt-in for email, a confirmation or “Double-Opt-In” is best for ensuring your communications are wanted.
- With SMS, opt-in can take place by:
 - A user sending a text to a keyword-shortcode combination, followed by a confirmation reply.
 - A user submitting a form on a website asking to receive SMS information of a particular type.
 - A user volunteering verbally on a phone call to receive SMS, which is then confirmed by the user when the first text message is received with a text reply.
 - A user submitting a form and opting in again as confirmed by a following text message/ reply.
- Records must be kept of opt-ins. Date/time of opt-in, method of opt-in, and confirmation are a minimum. Other relevant data may be important in case of a misunderstanding with a recipient.
- When soliciting an opt-in by any method, it's important that you clearly state the frequency and type of content the user will receive. For instance, if you receive and opt-in for appointment reminders, it's not OK to send messaging regarding new account services.

This is not an exhaustive list of rules by any means. For more information, please contact us for more reference material or advice on staying inside the lines with SMS.

LAWS/REGULATIONS – IMPORTANT HIGHLIGHTS

- Some parts of US Federal CAN-SPAM Act and the Telephone Consumer Protection Act have been ruled to pertain to SMS.
- The Children’s Online Protection Act covers collection of information from children under the age of 13 and covers the entire USA.
- The states of Michigan and Utah have their own, stricter rules for interaction and data collection from children, parts of which apply to SMS communications.
- Evolving “Do Not Track” legislation may have an impact on communications via SMS and/or mobile phone apps.
- mPulse is not a law firm and does not offer legal advice. There likely are other legal or regulatory requirements on your firm applicable to data collection or sending and receiving SMS and smartphone app messages. Please consult your attorney.

A NOTE ON THE MOBILE MARKETING ASSOCIATION (MMA)

Although your programs may be focused on general communications and not necessarily marketing via SMS, you need to be aware of the Mobile Marketing Association (www.mmaglobal.org). Over the years, the wireless/cellular carrier companies have come to depend on the MMA to communicate best practices in using SMS to interact with consumers.

There has never really been oversight by the government in how SMS may be used as a communication medium with consumers. As noted above, some of the laws and regulations pertaining to telephones and email apply, but SMS is in many ways unique and different.

Without oversight, the carriers have built up their own policies over the years on how SMS may be used to communicate through their networks. A major problem developed because different carriers sometimes have different rules about what is okay and what is not.

The Mobile Marketing Association has stepped into the role of a clearinghouse. Working very closely with the wireless carrier companies, the MMA has been successful in establishing and documenting acceptable use standards for SMS. Perhaps more importantly, the MMA has continued its founding tenet: representing the interests of businesses using SMS to send and receive messages. From its original role representing marketing interests, the MMA has expanded to encompass cross industry use and education, arbitration and evangelism of SMS, and mobile communications media.

For more information about best practices in mobile, use cases in healthcare and mobile messaging in general, please visit the MMA website.



IN-APP MESSAGING

The use of mobile apps to communicate securely with consumers is revolutionary in its ability to influence behavior and long term habits, save effort and time for the end user, and reduce overall costs for the healthcare organization.



Cases for implementing secure mobile communication via apps include:

- 1. User Habit:** Consumers have made the mobile phone a major part of their daily routine. Don't ask consumers to try using a new piece of hardware, reach them where they want to be reached. For example, a patient would rather communicate on their smartphone versus purchasing an additional medical device.
- 2. Data Security:** Two-way communications of PHI can now be provided to consumers by using a smartphone app.
- 3. Cost Reduction:** It is now possible to avoid unnecessary calls to a call center, nurse, or doctor by communicating routine PHI information via an app. A typical healthcare provider might pay \$1 per member per month in call center, print, and postage; for a provider with millions of members, this is a huge opportunity for savings.
- 4. Message Immediacy:** The smartphone app can prompt the user with an auditory and/or visual indicator on the phone to ensure timely delivery of important information and confirm that the user has seen the data. Ninety-five percent of text messages are read within 4 minutes. Push notifications (quickly becoming an alternative to SMS) are seeing very high rates as well.
- 5. Message Flexibility:** Smartphone apps not only send data but are also platforms for other activities surrounding the basic communications function. Data flow between the app and other healthcare or payer systems is facilitated and highly customized in the app.

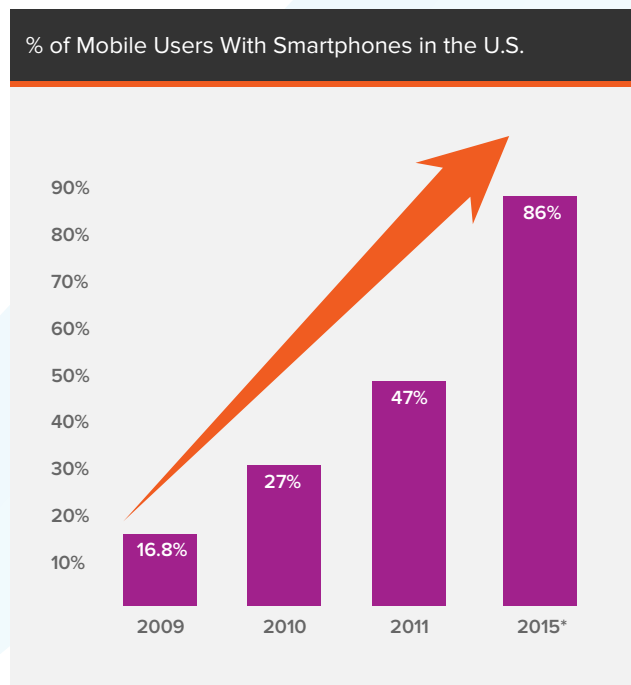
Why doesn't every healthcare provider and payer organization have an app to communicate securely with their members?

The simple answer is that since early 2010, it simply didn't make sense. You need a smartphone in order to run an app capable of encryption/decryption and password protection of PHI data to meet HIPAA and HITECH standards. Ownership of smartphones in the USA just wasn't high enough – a method of communication that can only possibly reach 10% of your audience is difficult to justify.

Well that has all changed! The outlook for smartphone ownership growth exceeded 75% in 2014 and will climb to over 85% in 2015. With over 1.25 billion smartphones being produced in the last 18 months worldwide, smartphone adoption will accelerate rapidly.

The outlook for smartphone ownership growth in 2011/2012 is strong; mPulse is predicting 47% of the U.S. will have a smartphone by the end of 2011, with an increase to 86% in 2015. If the cost is only \$49.99 for an iPhone, why wouldn't you want a smartphone?

Low consumer adoption was the barrier to using smartphone apps for secure or routine two-way communications. That barrier has fallen rapidly and has healthcare organizations scrambling to catch up to consumers.



*2015 prediction based on data from mPulse's [Mid-Year Mobile Marketing Report](#)

OPPORTUNITIES

Right now apps on smartphones are the most economical method of SECURE push communications with a wide audience. A smartphone app can be a single conduit through which PHI and non-PHI data can consistently reach targets.

The value to the healthcare provider/payer as well as the consumer is clear. Consider the following smartphone app capabilities currently being used and in development:

- Tracking apps allow the user to log information about his or her medical condition, status, or compliance to a care management regime. These apps compile the information on the smartphone, but more importantly can securely transmit data back to healthcare IT systems for ongoing assessment, retrieval, and alerting of the appropriate healthcare professional.
- Secure alerts with reminders about medication, exercise, and physical therapy appointments and reminders to check in with the app itself or healthcare professionals.
- Query/reply routines that ask a question and receive a response from the patient. Examples are post-surgical pain monitoring apps that prompt the patient to reply with a 10-1 comfort level, or a request for patients to take their blood pressure and enter the data to the app, which instantly sends it back to healthcare IT systems.
- Ongoing care management uses automated “workflow” logic, responding to patient interaction and input to the app. Based on patient input, the app can independently respond or communicate with healthcare IT systems to respond with encouragement, modified reminder frequency, updates, and milestones in condition management.
- Medical accounting, billing, and reconciliation information deemed to be PHI can be communicated directly through a smartphone app, with the ability for the plan member to get details, initiate a query, or even pay a bill.
- A smartphone app is ideal for video distribution of pertinent advice, instructional content, and healthy lifestyle encouragement and information.



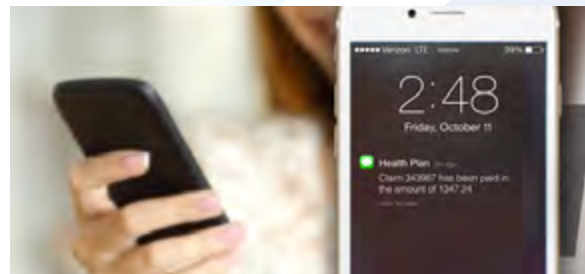
SMS MESSAGING

Using SMS, also known as text messaging, to communicate with members and patients has several special characteristics that make it an especially effective tool for healthcare organizations:

1. **Timeliness:** Over 95% of SMS messages are read by the recipient within 3 minutes of sending. Compare this to an email, letter, or even a call to a home phone.
2. **Interactivity:** SMS can be used for two-way communication with the recipient. A reply from the target can contain information routed to computer systems that can then apply a logic routine to determine if further action is required by a human or the program.
3. **Immediate Action:** An SMS message can contain a phone number or link to a secure website. Most cell phone users can click on a highlighted phone number in a text message to initiate an immediate call to a call center or particular person.
4. **Mobility:** Of course the biggest advantage to SMS messaging is that it can reach the targeted member almost anywhere at any time. The recipients don't need to be at home to take a call made to their home phone. They don't need to be at a computer to check email, and, even if they have email on their cell phone, most users check email infrequently and do not have email notifications activated on their phone.

SMS is great for general messaging in the healthcare industry. As a truly ubiquitous platform, it's very well suited if the information contained in the message is deemed a non-PHI application by the HIPAA obligated entity:

- Appointment reminders and rescheduling
- General medication and activity reminders
- Notifications such as HEDIS compliance encouragement that are relevant to broad groups
- Locations and wait time applications



The glaring limitation with SMS is that it can't be used to send PHI. As we've already discussed, there exists a broad and changing interpretation as to what constitutes PHI. But the fact remains that SMS is not a secure channel for purposes included in HIPAA guidelines.

ACCEPTABLE USES OF SMS WITH PHI IN HEALTHCARE

Almost all smartphones prevent a true SMS message from being received by any software other than a standard, proprietary SMS application that resides on the phone. This means that even if you're able to send 160 encrypted characters to a phone via SMS, it can only be received and read by the native SMS app. The native SMS app cannot decrypt the message, and it cannot be modified to decrypt a message.

Further, due to the architecture of the phone, a smartphone app cannot intercept, have forwarded, or in any other way gain access to a message sent to the phone via SMS. There are good reasons for this limitation if you are a carrier seeking to control the SMS channel.

There is no opportunity to use the SMS network to transmit PHI directly to consumers at this time, but there are a few strategies that have proven useful in leveraging the strengths of SMS as part of PHI communications.

- **Embedded Secure URLs** – Use SMS to alert a user when there is a message waiting on a secure website. Comscore reported that in December 2010, over 47% of mobile subscribers accessed and used the internet from their mobile phone. End-users enrolled to receive SMS alerts when secure messages are waiting don't need to constantly log-in to check if important news of lab tests, doctors messages, x-rays, or other services are available in their healthcare portal account.
- **Embedded Phone Numbers** – Direct users to “click to call” a call center, healthcare professional, or password protected voice message to retrieve important information that can't be transmitted in the clear.

PROJECT CONSIDERATIONS

Proof of Concept (“POC”) and Pilot Projects

Since not everyone uses the same terms for business processes, we are using the term “proof of concept” (“POC”) to mean a technical evaluation that includes an integration and implementation of part of the planned mobile functionality for your systems.



In contrast, we use the term “pilot” to mean evaluating of the social & business aspects of mobile-enabling your systems.

In many circumstances, the objectives of a POC and a pilot will need to be evaluated simultaneously. The nature

of your business will dictate whether you need to mobile enable your systems and software in order to test enduser acceptance of a mobile medium of communications from your products.

Proof of Concept

Using a proof of concept as an early step to integrating systems is a common IT process. We’ll presume that if you work for a company with a software product being sold to healthcare organizations, you have an established process for development. However, there are some aspects and milestones when mobile-enabling systems which are different or additional to a routine project.

When planning a proof of concept project to add mobile to your systems, please

consider the following points organized below as “General Mobile Advice”, “SMS Specific Challenges”, and “App Messaging Considerations”:

General Mobile Advice

Message Flow Mapping – In a proof of concept, you’ll want to test and understand how each message will travel from a trigger event to a resolution. First, map the process completely to determine what actions will be managed by your software, and what actions can/will be handled by outside systems.

Planning for Replies – Remember when mapping to include a means of handling a user reply or an acknowledgement that the message was successful delivered to the phone by the app or carrier. Also, plan for unexpected replies that don’t fit with the message map.

Test Groups – Choose a test group that can properly evaluate the POC. The test group should include people using a variety of device types and brands, and if possible, having different experience levels with mobile.

Context – When designing how your system will use mobile, remember the recipient’s context. Sending an email at 3:00 a.m. is no problem, but you don’t want to use existing email triggers to send an SMS message at the same time. Other context issues include asking whether the content is appropriate for SMS or App Messaging versus another medium. For example, short and simple for SMS is a must.

SMS Specific Challenges

Short code planning – Sending large numbers of SMS messages requires a short code. This is often “the long pole in the tent” in terms of a timeline for a proof of concept. A dedicated short code is one which is leased for use exclusively by your business. Dedicated short codes are often required due to security and branding considerations. Obtaining and provisioning a new dedicated short code can take 12 weeks and longer. A shared short code can sometimes be used for testing purposes, or your mobile partner may be able to lend you a short code for low volume testing.

Two-Way Nature – One of the best aspects of SMS is that it's two-way. Interaction can be initiated by a cell phone user or by your software, and may continue for several exchanges. We've found in our experience that establishing a successful system for sending messages OUT is far easier and faster than configuring your systems to receive and process inbound messages. If possible, consider a phased approach to test outbound functions quickly, and then move to inbound applications.

Unexpected Replies – Expect to receive replies or consumer initiated texts that do not fit established message flows. Establish and review an SMS inbox continuously to tune your system's logic to handle a wide variety of messages inbound to your application.

Character limits – Subject to opt-in requirements depending on the type of message you are sending, you have between roughly 140 and 160 characters in a single SMS message. While in a proof of concept, it's important to understand if each type of message you'd like to send can be contained in this envelope.

App Message Considerations

App Distribution – Depending on your business, you may be considering a standalone app or establishing messaging to existing apps already belonging to your clients.

App Security Strategy – If you plan to send PHI data to your app, or to send messages to your app distributed by your client, you need to decide how the message will be secured. Encryption/decryption utilities and message management capabilities are built into several commercially available Software Development Kits (SDKs).

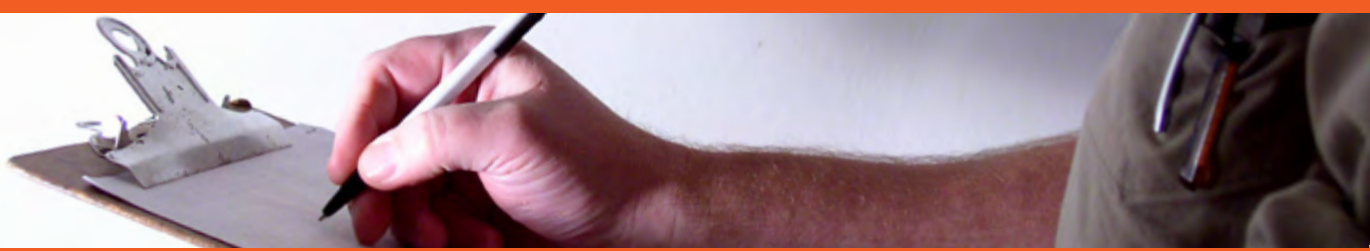
Messaging Systems – Suppliers of these SDKs may be able to offer supporting software and systems that you can use to reduce development time in your systems and applications. mPulse for instance extends functionality of its online, multi-channel platform through APIs leveraging its SDK to provide secure/encrypted messaging.

Pilot Projects

Many businesses contemplating the addition of a mobile component to their systems and software face a fundamental question: Do the end-users of my product want the service? If you suspect that mobile communications would make a good addition to your product but are unsure of the level of acceptance, a pilot project may be in order.

In a pilot, the emphasis is on verifying end-user acceptance of SMS or smartphone app-based communications with your audience. A pilot will help you determine:

- **Acceptance:** How do end-users feel about being sent SMS messages? Are they willing to download an app to their smartphone? What is the real percentage in your end-user universe that can and will use a mobile app to communicate with your systems?
- **Volume:** How much messaging will occur when your systems are fully mobile-enabled?
- **Costs:** What are expected volumes of messages, and what are the direct and indirect expenses involved in communicating via this new, additional medium with users.
- **Value:** Your end-user audience is interested and accepting, but is it perceived as having enough value to justify the potential expense to you and your customer?



A CHECKLIST FOR CONDUCTING A PILOT

- ❑ Plan a resource commitment for the pilot. At minimum, a single project manager should be assigned to work with vendors and consolidate/distribute information to stakeholders.
- ❑ Plan a personnel commitment for the pilot. In addition to a project manager, a thorough pilot project may consume one or more people on your staff for several weeks or months.
- ❑ Depending on the variables you want to test and the complexity of your plan, you should expect to invest focused resources for a complete evaluation. Your mobile partner or other vendors may be able to augment your staff.
- ❑ Have a measurable plan. The biggest reasons a “test” fails is a lack of clear objectives and/or not having the correct measurements in place. Plan to declare victory at the end of the pilot, or at least have conclusive data about what happened.
- ❑ Limit and categorize the programs you’ll want to try. Organize them in three sets:
 - ❑ **First Priority:** Choose 1-2 programs to launch ASAP. These should be the programs you feel are simple to deploy and most likely to achieve results. For instance, this may be a program to provide simple health reminder alerts to a group of similar end-users.
 - ❑ **Second Priority:** After you have a good feel for the first set of programs, consider expanding to 1-2 others to find out if they perform better or worse than the first set. You now have learned enough to be able to give the less obvious programs a better chance of success. Measurement, as always, is a must.
 - ❑ **Third Priority:** Choose message flows that you’d like to try, but perhaps the success or failure of the pilot doesn’t depend on. You may not get to them during the pilot period, but then, you may have a good idea of their probability of success.



PILOT PROGRAM TIPS

1. Only pilot what you can measure. If you can't measure it, you won't understand the investment. That is the point of the pilot!
2. For the pilot, choose programs that can be easily measured inside the pilot term and that do not have to extend beyond the pilot. Loyalty programs or ongoing alerts that people may come to depend on are less desirable in a pilot. If you need to pilot programs that are of ongoing interest, make sure to be very clear that you're conducting a pilot and that the alerts may be discontinued.
3. Mobile app development can be very expensive for just a casual try. Consider limiting your piloted app to a simple, secure messaging function, and communicating clearly to endusers that there is more to come.
4. If a program requires heavy integration with other systems it may not be appropriate for a pilot. Simplify the integration by using a hybrid that includes manual processes to simulate the messages you will be sending and receiving.

DURING THE PILOT

- Set a regular schedule to review results with stakeholders on the project. This includes:
 - The project manager
 - Managers who will benefit from the results
 - Partners or vendors in the project
 - Users of the product
- Have measurements consolidated into a dashboard
 - Tip: Watch "unsubscribe" rates and rates of reply & input to the app to measure how well your audience is engaged
- Don't just stand there! Modify and tweak the program after it has time to give you

relevant data. Change:

- Frequency of communication,
 - Method of communication,
 - Types of communication offered,
 - And, as always, play with your messaging a bit to optimize.
- Plan for success as the pilot progresses and for what you will do when the pilot is finished.
 - Do you need to add human or IT resources?
 - Was there something you missed that is now obvious to you?
 - Do you need another measurement to be sure you are capturing the right results?

AFTER THE PILOT

- If it makes sense to continue with programs you've piloted, DON'T let there be a lag time. Keep up the momentum, or you'll lose ground on your database, end-user interests, and result.
- vHave a debrief meeting with your stakeholders and identify:
 - What went well? How can you replicate results?
 - If something went wrong, do you know exactly why it did and how you can fix it (and what would happen if you did fix it)?
 - What are the projections if you press the gas pedal right now?



CHOOSING A MOBILE PARTNER

A Google search for “SMS Marketing” will turn up hundreds of businesses that sell SMS services. Mobile phone app companies are also springing up at an astounding rate. Based on what our clients have told us, there are few companies in the US capable of supporting major software integration at a professional level in mobile. Of those, only a handful are focused on the healthcare market to the point of understanding and complying with healthcare’s specialized requirements.



In working on many projects with our clients, and in responding to dozens of very thorough RFPs, we’ve come to understand some of the most important considerations in deciding what kind of mobile partner can best support your business.

Here are some of the questions we feel are important to answer:

- Does the vendor have consistent internal processes in place to avoid “channel-conflict” or cross messaging to your clients?
- Is the vendor’s infrastructure and organization HIPAA-compliant? Is it able to sign a business associate agreement and pass audit (if required)?
- Does the vendor have a professional project management team and processes in place to support a modern development cycle?
- Does the vendor have direct experience supporting businesses that use their messaging as part of an overall solution? What kinds of support choices are available?
- What documentation exists on application programming interfaces (APIs)? How thorough is the documentation?

- Are standard application-exchange protocols such as SOAP/XML used in the APIs?
- Can the vendor handle the volumes of data you are expecting?
- Is the vendor's business stable and in a position to support you and your clients for the foreseeable future?
- Is there a cultural fit between the vendor's staff and yours? Will they communicate?





ABOUT MPULSE



mPulse mobilizes the consumer experience by making healthcare communications relevant to the modern lifestyle. We utilize complex mobile technology to provide simplified, streamlined solutions that enable health partners to effectively connect with consumers in the most relevant and appropriate means. By improving communication, we aim to improve the health and wellbeing of consumers everywhere. For more information, visit mPulseMobile.com, formerly a MobileStorm company.

Find out more by visiting

www.mPulseMobile.com

sales@mpulsemobile.com

mPulse Mobile Inc.

16530 Ventura Blvd. Suite 502

Encino CA, 91436

Telephone (805) 200-4848

www.mPulseMobile.com

