mHealth: How Mobile Apps Can Help Health Plans Improve Consumer Engagement and Facilitate Behavior Change
INTRODUCTION

The ubiquity of mobile devices seemingly knows no bounds. Nearly every person today is using a mobile device to check email, surf the Web, update social networking profiles, play games, shop online, watch videos, chat with friends, pay bills, and more. In fact, more than 130 million people in the United States now own a smartphone, and these devices have become so embedded in society that “44 [percent] of cell owners have slept with their phone next to their bed because they wanted to make sure they didn’t miss any calls, text messages, or other updates during the night.” The tablet population is also growing: More than 30 percent of Internet-enabled households in the United States now have a tablet computer.

As consumers’ use of mobile devices has increased, so too have the promise and importance of mobile health (mHealth) applications. The Pew Research Center reports that half of all smartphone owners use their mobile device(s) to obtain health-related information, and one-fifth have installed at least one health-related app. This extensive adoption of mHealth offers payers, providers and consumers a new model for engaging with each other, and can promote a more meaningful relationship and exchange of information between parties. This new form of consumer engagement is particularly important for healthcare payers as they look for ways to improve member satisfaction, loyalty and retention. mHealth can be a key strategic weapon for payers facing mounting pressure from rising medical and administrative costs, the uncertainty of healthcare reform, the implementation of public/private exchanges, and the threat of disintermediation from accountable care organizations (ACO) and provider-led health plans.

Aetna’s acquisition of i2t, Humana’s partnership with Vitality, and the number of payers that now have mobile apps in the Apple and Android app stores show many payers are starting to embrace mHealth fully. However, to maximize their investments, they need a comprehensive mHealth strategy. They also must take care in how they deploy these capabilities, so as not to deliver a poor user experience or risk the loss of sensitive information. Simply moving self-service capabilities, especially those rarely used, from a website to a mobile platform will not keep members engaged.

When developing a comprehensive mHealth strategy, a healthcare payer needs to consider the following:

- How can I maximize mHealth to optimize member engagement and facilitate behavior change?
- How can I provide a secure environment for the exchange of sensitive personal information?
- How can I integrate mHealth information into existing workflows?

MEMBER ENGAGEMENT AND BEHAVIOR CHANGE

Mobile devices are a fast, convenient way for members to access self-service information such as provider directories, benefit summaries and coverage, formulary information, and claims information. Healthcare payers like Florida Blue, for example, have implemented “click to connect” functionality on their mobile apps so members can access customer service when they need it.

The key to successful customer engagement is to provide high-value, personalized information at the time of need. But too often, payers use their web or mobile apps as a way to reduce administrative costs, instead of looking for ways to better engage customers. Reducing administrative costs is an important element, of course, but pales in comparison to the potential healthcare and sales value that could be derived from such initiatives. To optimize member engagement through mobile technology, payers must look to lessons learned by other industries, like retail and hospitality.

Mobile technology is used for information verification as well as easy access to immediate assistance during a point of decision-making. Such a need is even more acute for healthcare organizations, as access to information and help in moments of need is critical. This interaction will facilitate a healthy and trusting relationship between healthcare plans and their members.

Mobile devices and health-related apps are being used to positively impact and influence a member’s health status. For example, mobile devices provide an effective way for users to track healthy behaviors such as exercise programs, daily nutrition logs, medication compliance, and critical test scores, like blood pressure readings. This information should be integrated into a payer’s traditional care management programs, providing clinical staff with valuable insights into member behavior and health status.

With members’ consent, clinical staff also can send tailored mobile messages to keep users engaged; instantaneously modify users’ care plans to respond to daily changes; or determine when a member should be contacted and advised to seek medical help. Mobile devices also serve as another channel for payers to send care plan reminders, collect health risk assessments survey data, provide cost and quality information, and deliver information to members about preferred providers.

Payers also need to compose engaging mobile communications for users. But too often, communications are written by clinical staff using clinical terminology. One mHealth company that is taking a different approach with mobile communication is Sensei Health. It employs writers with various backgrounds (e.g., clinicians, comedians, teachers) to compose several versions of a standard message. Sensei then tracks a user’s response rate to each message type and sends future communications in the style that generated the highest rate.

INFORMATION TECHNOLOGY

IT department discussions typically center on whether to buy or build a capability. However, prior to determining sourcing strategy, both the business and IT departments must come to an agreement on the company’s long-term mobile strategy. In addition to the business aspects, this strategy must address three important elements: privacy, security and application platform. See the following sidebar for technical details regarding these three elements.

---

1 Sensei Health: www.sensei.com.
IT Considerations for mHealth Programs

Mobile Privacy

In order to maximize the benefits of mHealth, users must be comfortable that their personal and protected health information will be handled in a confidential and ethical manner. “Health information privacy is an individual’s right to control the acquisition, uses, or disclosures of his or her identifiable health data.”

mHealth poses many challenges to user privacy due to the large amount of medical data that can be collected over a prolonged period of time, an increase in the number of sources and types of data that can be obtained, and the large network of resources that can be granted access to a user’s confidential data.

To address these new challenges payers should follow a common privacy framework such as the Office of National Coordinator for Health Information Technology (ONC) Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information or the Markle Foundation’s Common Framework. These frameworks address the nine core principles of privacy protection.

1. Openness and Transparency
2. Purpose Specification and Minimization
3. Collection Limitation
4. Use Limitation
5. Individual Participation and Control
6. Data Integrity and Quality
7. Security Safeguards and Controls
8. Accountability and Oversight
9. Remedies

Greater transparency and consumer choice are critical while the technology standardizes in the market. Extending choice and control to members on the type of information being shared and educating both users and providers on best practices are keys to overcoming these challenges.

Mobile Security

As transactions are moved from traditional computers to handheld mobile devices, including tablets, the need for enhanced mobile security has increased dramatically. The three major mobile operating systems (OS) – Apple iOS, Google Android and Microsoft Windows Mobile – have enhanced their native security features. But if users are sharing electronic protected health information (ePHI) on their mobile platforms, these native features are not enough. Application developers therefore must take additional steps to ensure user data is secure. They also must address user authentication, in-app controls, ePHI data storage, logoff procedures, and remote wiping. These additional precautions will help ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA) and other government regulations.

The first step to securing a user’s ePHI is to verify the user’s identity. With devices often shared among family and friends – and easily lost or stolen – the application must have a secure and thorough logon and authentication process.

A multifactor authentication (MFA) process can be especially effective. It requires a user to enter additional data beyond the standard username and password. MFA often incorporates additional knowledge, possession, or inheritance factors such as personal identification numbers (PINs), physical or virtual tokens, and/or biometrics.

---

(Note: When designing this type of feature, care must be taken to ensure data security while avoiding a burdensome sign-on process that may lower utilization.)

Most mHealth apps allow users certain freedoms, such as the ability to interact with social media sites, take screenshots, or print information. Disabling these functions for an mHealth app will prevent the accidental transmission of ePHI to unintended recipients, and can keep users from inadvertently posting their glucose or blood pressure readings on social media platforms such as Facebook.

Mobile devices and apps also have the ability to store critical health information, which obviously presents a potential data security risk. If transmitting ePHI, the mHealth app should be carefully configured not to store data on the local device. Instead, the device should simply be used as a reader for the ePHI information that is stored on a secure, remote server. If ePHI is stored on the device, remote wiping features should be deployed in case the mobile device is lost or stolen.

mHealth apps also should deploy an automatic logoff function that ends the user’s session when the app is closed or following a period of inactivity. This ensures data will not be viewable to the next user of the device.

Application Platform

Whether developing your own mobile capabilities, sourcing them completely to a third party or using a hybrid approach, a carefully constructed Mobile Enterprise Application Platform (MEAP) should be used to allow a payer to write once and deploy/run everywhere, versus a native application developed for each OS. A single native app can provide a good user experience, and interfaces no doubt will take full advantage of native device capabilities. However, the development team will need to create and maintain apps for each mobile platform (i.e., Apple iOS, Android, Microsoft). Initial costs may be low, but recurring maintenance costs are high and will serve to complicate the future delivery of new capabilities across multiple platforms.

An appropriately structured MEAP approach can still provide a positive user experience and user-friendly interface, while allowing IT teams to develop once and deploy across all mobile platforms. Applying the “Rule of Three” also can be valuable when determining whether and how best to deploy a MEAP architecture:

- Will your solution support three or more mobile applications?
- Will your solution support three or more mobile OS?
- Will your solution be integrated with at least three back-end data sources?

If the answer to these questions is “yes,” then it’s best to implement your organization’s mHealth initiatives using a MEAP architecture.

It also is critical to consider privacy issues related to the technical aspects of the application and architecture. Will we require ePHI to establish a link? What ePHI does the customer/patient want to see? Do we need to display as much ePHI as we currently do? If there is a problem with the data validity, will we assign a contact for the patient to have the data corrected if it is wrong? These are among many security- and privacy-related questions healthcare organizations should address.

Regardless of the approach selected, it’s important for IT departments to avoid the “not invented here” trap. While developers love to tinker with new capabilities, the strategic risks might be too great to depend solely on internal solutions – and humility and prudence might dictate alternative approaches.

---

7 MEAP, a term first coined by Gartner in a 2008 Gartner Magic Quadrant report, is widely used in the mobile space today. A MEAP approach is intended to help organizations address challenges that can arise throughout the development, deployment, and life cycle of a mobile solution.

8 The “Rule of Three” in mobility, a concept introduced by Gartner, is widely used to describe the practice of applying a long-term, comprehensive, and strategic approach to launching mobile solutions.
WORKFLOW INTEGRATION

Now that you have acquired vast amounts and varying types of customer data, the challenge becomes turning that data into usable information with which you can make informed decisions. The key is to present the information in a manner that allows end users (clinical staff, customer service, marketing teams, etc.) to better support customers. Often this data is dumped into a large spreadsheet and the end user is left to figure out how to make sense of the data. Payers must give careful attention to how they ingest, process and present the data.

The information must then be integrated into a payer’s existing workflow in the form of actionable data. The information should guide next steps for care management, customer service, sales and other departments to ensure they are providing an optimal customer experience.

Collecting data for the sake of having more data makes no sense. Payers must collect the right data in the right way and convert it to actions that allow them to respond effectively to a user’s needs and preferences and help effect meaningful engagement and behavior change.

CONCLUSION

We are still on the leading edge of figuring out all the uses for mobile technology in the healthcare space. But we all can agree that mobile technology has the promise to drive transformative change in healthcare as it has in other industries, including banking. Yet many healthcare payers are only in the earliest stages of mobile technology adoption; some are still only thinking about making the move. To achieve transformative change, healthcare payers need to be more proactive and strategic about developing mHealth initiatives. A well-designed mHealth strategy not only can play a key role in a payer’s business processes, but also in its broader member engagement strategy.

As mHealth capabilities grow and evolve, so, too, does government oversight of these capabilities. In 2013, the Food and Drug Administration (FDA) released guidelines for mobile medical applications to identify the subset of mobile apps that will require FDA approval. Mobile apps that function as medical devices and whose functionality could pose a risk to patient safety if the mobile app were not to function as intended will require FDA approval prior to being publicly available. Most mobile apps available today do not pose a risk to the public and, therefore, would not require FDA approval.

As your organization embarks on the mobile health journey, it is important that you understand the benefits and risks. You must integrate mHealth information into your organization’s existing workflows in a thoughtful manner, and select a path that will enable you to enhance your customers’ experience while ensuring their information is managed in a secure environment.
ABOUT PROTIVITI

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 40 percent of FORTUNE 1000® and FORTUNE Global 500® companies. Protiviti and its independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

About Our Healthcare Solutions

Protiviti’s healthcare specialists partner with commercial and Medicare Advantage payers, state Medicaid programs, pharmacy benefit managers (PBMs) and health services companies to maximize opportunities in the changing healthcare landscape. Protiviti brings deep industry knowledge and skills to help healthcare organizations design, build and execute strategic initiatives while effectively managing risk.

From members, employers and providers to regulators and investors, healthcare companies must delicately balance the competing demands of their many stakeholders to succeed. They must develop and deliver innovative solutions and seamlessly manage a business that involves frequent change. And they must identify and manage the business opportunities and risks associated with this dynamic environment.

At Protiviti, we are in the business of developing and delivering proven solutions. We know how to manage change effectively and efficiently. We partner with our health plan clients to bring deep skills and proven methodologies to bear on the problems that matter. In doing so, we help our clients gain a competitive advantage and satisfy the competing demands of their many stakeholders.

For more information, visit www.protiviti.com/healthcare-payer.

Contacts

Susan Haseley  
+1.469.374.2435  
susan.haseley@protiviti.com

Earl Rousseau  
+1.404.443.8223  
earl.rousseau@protiviti.com
# Protiviti Locations

## THE AMERICAS

### UNITED STATES
- Alexandria
- Atlanta
- Baltimore
- Boston
- Charlotte
- Chicago
- Cincinnati
- Cleveland
- Dallas
- Denver
- Fort Lauderdale
- Houston
- Kansas City
- Los Angeles
- Milwaukee
- Minneapolis
- New York
- Orlando
- Phoenix
- Pittsburgh
- Portland
- Richmond
- Sacramento
- Salt Lake City
- San Francisco
- San Jose
- Seattle
- Stamford
- St. Louis
- Tampa
- Washington, D.C.
- Winchester
- Woodbridge

### CANADA
- Kitchener-Waterloo
- Toronto

### ARGENTINA*
- Buenos Aires

### BRAZIL*
- Rio de Janeiro
- São Paulo

### EUROPE/MIDDLE EAST/AFRICA

### FRANCE
- Paris

### ITALY
- Milan
- Rome
- Turin

### THE NETHERLANDS
- Amsterdam

### BAHRAIN*
- Manama

### QATAR*
- Doha

### UNITED ARAB EMIRATES*
- Abu Dhabi
- Dubai

### SOUTH AFRICA*
- Johannesburg

### ASIA-PACIFIC

### AUSTRALIA
- Brisbane
- Canberra
- Melbourne
- Perth
- Sydney

### INDIA
- Bangalore
- Mumbai
- New Delhi

### INDONESIA**
- Jakarta

### JAPAN
- Osaka
- Tokyo

### SINGAPORE
- Singapore

### SOUTH KOREA
- Seoul

### ** Protiviti Alliance Member

---

* Protiviti Member Firm
** Protiviti Alliance Member

---

© 2014 Protiviti Inc. An Equal Opportunity Employer M/F/D/V. PRO-PKIC-0514-139
Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.