Intertek

Valued Quality. Delivered.

Top 6 Failures in mHealth Apps

Background

The infiltration of apps into everyday life—and everyday healthcare—has fostered new opportunities for traditional medical device manufacturers and non-medical businesses alike. The widespread adoption of mobile devices among healthcare professionals in particular has become commonplace as it supports the exchange of health data in real time and at the point of care.

With the U.S. Food and Drug Administration's (FDA) recent draft guidance outlining its approach to general wellness medical apps and medical device accessories, the number of mobile health apps—or, mHealth apps—entering the $2.8 trillion-U.S. healthcare market is exploding. But many of these medical apps—whether intended for the low-risk consumer market or the moderate- to higher-risk professional healthcare market—suffer from common development issues. This white paper offers clarification, information, and explanation on top failure issues our experts frequently come across in regards to mHealth apps. It also seeks to offer information on what medical device manufacturers and app development companies can do to not only head off any issues in the creation of a new mHealth app, but also how to potentially address them in existing apps as well.

Information Safety and Security Concerns

Nearly all apps contain data that users would consider personal—names, locations, and the like—but mHealth apps typically are collecting data that can be considered much more sensitive. From blood pressure readings to heart rate monitorings to EKG readings and beyond, health data is inherently very personal to people, and the vast majority of mHealth app users work to keep that information between themselves and their relevant healthcare professionals. Thus, one of the largest issues with mHealth apps deals with is keeping this personal health data safe and secure.

HIPAA is the federal Health Insurance Portability and Accountability Act of 1996 and part of its directive is to protect the confidentiality and security of healthcare information for patients in the U.S. while also allowing patients more rights with their own individual information, including enough disclosure needed for patient care. Also, in focusing on the business aspect of the law, according to the U.S. Department of Health and Human Services website, the HIPAA Security Rule "specifies

Potential HIPAA Medical App Errors

- **patient data left unsecured**
- **personal health records shared without permission**
- **manipulating or exploiting user collected health data**

a series of administrative, physical, and technical safeguards for covered entities and their business associates to use to assure the confidentiality, integrity, and availability of electronic protected health information."

To help validate HIPPA compliance, testing to know where an app's data transmission may be vulnerable is highly necessary. While it is true that no matter how much security testing is executed there is no guarantee that an app will be immune to hackers and other malicious visitors, it is guaranteed that with the right kind of security testing and protection implemented, an app will be less likely to suffer a targeted attack, and the implications for app users, and the associated brand, will be significantly reduced.

Lack of In-app Security

App development companies also need to create policy determining how an mHealth app will deal with issues of security within the app itself. This can include PIN/password access and lockout capabilities, but also how the mHealth app interacts with other on-device apps. Obviously there can be legal implications regarding HIPAA laws and confidentiality here, but in-app and on-device interaction issues also can significantly affect user satisfaction.

For general wellness apps, allowing users to manage their data how they want within an app is highly necessary. Users should be able to categorize or delete data without worries about that data reappearing elsewhere or being stored somewhere within the app or on the device in a way that is unknown to users. Thus, the development company must allow them to deal with the collected health data on an app any way they see fit, including the secure deleting of data from the app and the device entirely.

This can be difficult for both lower-risk wellness apps and higher-risk health apps when an mHealth app is interacting with other apps on a device too. Is that other app storing information it should not be about the health data of the user? And how are other apps on the device communicating and using such information? For example, many mHealth apps interact with social media apps or mapping apps—but should they? Do all users want their blood glucose readings or EKG updates to immediately hit their social media feed? Should the use of an mHealth app affect the data populating an Internet search on a smartphone? Users must be allowed to make decisions about how their data is populated and displayed within other apps. Weak policy regarding on-device sharing also can make it easier for an app to be hacked or for user data to be stolen elsewhere, leading to much more significant issues.

Privacy Policy Gaps

In light of the significance of potential HIPAA issues with an mHealth app, the company and its developers need to be prepared with the proper development materials and policies. Given the sensitivity of the data mHealth apps collect, clearly a privacy policy is paramount.

In the past, some mHealth app development companies have simply repurposed privacy policies that were well-written documents created for different companies, products, and/or brands. Although the creation of a sound privacy policy can take some work, having a document drafted that specifically pertains to your exact mHealth app and all its associated needs lead to a stronger product.

A good privacy policy addresses any issues particular to a specific mHealth app, as well as information on how the app and the development company will collect and store user data, how said data will be used for the company's and others' purposes, when the data will be used, if the data is being manipulated at all, and so on. Having such a document shows users the transparency of a company's intentions, as well as helps provide protection in the case of any adverse issues. Additionally, in devising how an mHealth app interacts with other app and programs on-device, the company and its developers are figuring out, in part, the privacy policy for an app. Information about data sharing and the app's interactions with other programs and apps should also be spelled out.

For these reasons, app development companies should not just pick up the policy of another medically concerned company, app, device, or product. While potentially meeting most of the needs of a particular mHealth app, there is no way a policy that wasn't devised specifically for a particular app's functionality can cover all the needed security, privacy, and data management issues.

Lack of Physician or Subject Matter Expert Involvement

In the development of many mHealth apps historically, the involvement of a physician or a subject matter expert in the app's creation has sometimes been considered an afterthought. While traditional medical device manufacturers are well-accustomed to turning to professional healthcare providers for device design and development expertise, new healthcare market entrants with little or no medical experience may not be seeking out the correct expertise on an app's abilities and functionality, connectivity and interoperability, display, communications, and more. App developers have extensive coding and programming skill they are intensely putting to work in the creation of an original mHealth app, but if they are turning to simple Internet research or general knowledge to help develop the actual functionality, they are almost certainly missing necessary input.

In order to ensure the efficacy and reliability of any data taken, monitored, or stored in mHealth apps, physicians and/or medical experts must be involved from early on in the development process. Having a medical expert involved from early stages is one of the only ways to ensure each aspect of a health-associated product is considered and addressed correctly according to the needs of the app and its users. Are the correct units of measurement being used? Is the timing correct? Are the colors the app uses signifying the correct attributes that medical professional and/or patients are familiar with? And how are the app development companies ensuring the readings the app is giving are accurate? What could users potentially read into when they see these results?

This type of efficacy verification and testing goes beyond seeing if an mHealth app does what it says it does and that it displays a result that seems accurate when used. It is about how that data is and can be interpreted within a health, wellness, and medical context. Development-level input from physicians and medical professionals helps negate everything from simple to elaborate mistakes, as well as ensure the information being conveyed is within accepted physician parameters and that the collection methodology and display is correct.

Some app development companies focus on the programming and coding only in the upfront development, deciding to not bring in a medical expert to verify their app's offering until late stages or until they decide to push their app through with an FDA 510(k) clearance. However, having medical and testing experts involved from early on means avoiding costly mistakes later. It can mean catching errors, which would otherwise require days or weeks of reprogramming, before they become an issue. It also helps reassure the development team and, eventually, the users that the mHealth app they are getting has the correct medical expertise behind it. Creating an app that works in the correct way with the correct connotations and the ability to share accurate results is much easier to push forward than an app that will require fixes or maybe even an overall revamp further down the road.

Expected and Unexpected Usability Issues

Ensuring the safety of the data collected by and housed in an app is incredibly important, as is developing the app with the correct expertise and knowledge behind it. However, if users can't easily get to or utilize the data they're collecting and storing in an app because it proves difficult to navigate or handle, that can cause just as much, or possibly even more, trouble.

Usability testing is a distinct and crucial part of an app's development. If a user finds, for example, that an app's readings aren't clear, or that storage retrieval isn't easy, if any of the buttons are too close together or too difficult to push, if data, results, and readings are unreliable, or if there are areas of the app that are difficult to get to or to utilize properly, users can just as simply drop using this particular mHealth app altogether. This also may be an opportunity to work with a UI (user interface) expert who can advise on how users will actually utilize an app as opposed to the idealized interactions established by the developers. User-centered design helps bring focus to the development of the experience, ensuring user interactions with the app bring value and significance to the product.

As an extension of usability, there likely will always be issues app developers, subject matter experts, and others on the development team did not think of in the creation of their product. There is never a guarantee that users will use the capabilities of the app in the fashion in which they were intended and designed. Unexpected use cases will appear and while those can range from easily fixable to potentially dangerous, mHealth app creators need to know as much as possible before launch.

What would happen if the app malfunctions in the middle of a blood pressure reading, for instance? Would the data be stored differently? Would the user be notified? Are there backup contingencies or alternate use scenarios? Or, what if a user it utilizing a feature in an unintended way, such as using a notes feature to record data that is not being collected by the app? How does that affect readings, or storage, or the performance of other aspects of the app? What if an app tries to sync with an unsupported Bluetooth device that a developer never intended? Would the sync cause an unintentional broadcast of private data? Are there restrictions put in place to limit such possibilities? Testing to see ways users may interact with an app beyond simple usability can be key in development, as it brings insight to not only usability but also to new potential errors or user pitfalls that might be dangerous.

Obviously, there is no way to stop all types of negative use cases, but mHealth app developers and their companies must be aware of as many alternate or unexpected use scenarios as possible in order to set parameters with the app to help address any issues these scenarios could cause. In addition to security and usability implications, unexpected use can have an impact on everything from performance to battery usage to functionality. The more development companies know and can predict about the use of their mHealth app, the more they can optimize and modify it and its performance to offer the best possible user interactions.

Lack of Regulatory and App Testing Knowledge

The regulation of health and wellness apps is currently in a state of fluctuation in the U.S., but apps that are specifically deemed as medical are governed by the U.S. Food and Drug Administration (FDA), under its 510(k) and Premarket Approval (PMA) regulations. If the FDA feels an app has crossed over into medical territory, it must be prepared to adhere to the necessary regulations and stipulations, or subsequent action can cause the app to be pulled from the marketplace altogether.

For example, a urinalysis app called uChek, created by India-based company Biosense Technologies Pvt. Ltd., drew the FDA's attention when it launched in the U.S. market in early 2013. The app claimed it could help users determine their risk for more than 25 medical conditions by taking a photo of a utilized urinalysis chemical strip and then using that photo to make medical color analysis comparisons. According to a letter from the FDA to Biosense Technologies, the dipstick strips associated with the uChek app had achieved the proper FDA clearance, but the app used to analyze, read and interpret the results of the dipsticks had not obtained proper FDA clearance.

Consequent to this letter, Biosense Technologies pulled that iteration of uChek from U.S. availability and launched an online crowdfunding campaign to help it gain capital and user data to support its work in achieving the proper FDA clearance.

Typically, when the FDA makes this type of move, they meet with the app developer and urge them to put their product through the 510(k) clearance submission process, which aims to ensure the developer followed the proper guidelines in the development of a medical application. This typically requires the inclusion of at least third party-conducted and -verified studies and data, if not full-on clinical trials, as well as documentation on how the app shows substantial equivalence to a current medical device.

Other factors that can push apps into needing FDA 510(k) clearance would be if they communicate and/or interact with a medical device such as (but not limited to) a pacemaker or an insulin pump, as well as if the app is making claims that it is equivalent to using a medical device that has achieved 510(k) clearance.

Development is the time to know an app inside and out, and the best way to complete that knowledge is through third-party testing. Developers intimately know their apps—and it is necessary to take a run at them with someone who doesn't. What can an everyday user make work, and what can they not find? Where are there potential vulnerabilities? The answers to these questions, which can only be found through third-party testing, bring the strongest possible product to market launch.

Third-party testing also is an opportunity to get true user experience with an mHealth app on a range of different devices and networks. As newer generations of smartphones and tablets continually hit the market, development companies have to make sure their apps continue to work well with this new technology—as well as with the old technology. Testing can help development companies see where improvements or patches need to be made in order to maintain app usability and security, regardless of what device a customer is on.

When it comes to mHealth apps, testing early and testing often is one of the most cost-effective and efficient ways to develop and maintain a quality product. That may sound counterintuitive, considering that testing costs money and takes time. However, when comparing the differences in cost and time between testing early in the development process versus correcting mistakes and battling a negative public image after release, there is no denying that being proactive saves time and money.

Additionally, third-party testing experts can bring their knowledge of standards, regulations, industry changes, and more to a project to help create an app that is much more likely to see success in the marketplace. Regulatory approval can provide a competitive edge, as it promotes that consumers and medical professional alike can trust the app, and market acceptance is a key factor in an app's ultimate success. Partnerships marrying app product development with regulatory expertise are best positioned for success, and when necessary testing is not available in house, seeking a software testing organization with robust capabilities and knowledge of the medical market, its regulations and intricacies, and its evolving structure is the smartest play.

There currently are very few mobile medical apps that have acquired FDA 510(k) clearance, due primarily to the much more stringent requirements. Having FDA 510(k) clearance can help heighten the perception and marketability of an app, but it also does require a much more significant time and monetary investment on the part of the app developer. Additionally, the FDA and the federal government continue to monitor this section—and intersection—of the mobile and medical businesses, and app development companies should be aware that more restrictions and requirements could be imposed onto mHealth apps at any time.

Conclusion

According to a recent report from PricewaterhouseCoopers, 86% of clinicians believe mobile apps will become more important to physicians for patient health management over the next five years. With this kind of increasing interest, the spotlight will only glow more hotly on mHealth apps. Now is the time to address issues in development and implementations. By knowing potential pitfalls, what to watch out for, and what to pay closer attention to, mHealth app development and traditional device companies can create more robust, more useful products that will help give users the health experience they want and help give their businesses a brighter future.

About Intertek

Intertek is a leading quality solutions provider to industries worldwide. From auditing and inspection, to testing, training, advisory, quality assurance, and certification, Intertek adds value for its customers by helping improve the quality and safety of their products, assets, and processes. With a network of more than 1,000 laboratories and offices and over 36,000 people in more than 100 countries, Intertek supports companies' success in the global marketplace by helping customers to meet end users' expectations for safety, sustainability, performance, integrity, and desirability in virtually any market worldwide. Visit www.intertek.com.

To connect with an expert on this topic, or to discuss a new project, contact your local Intertek at 1-800-WORLDLAB (967-5352), via email at icenter@intertek.com, or on www.intertek.com/mobile .

This publication is copyright Intertek and may not be reproduced or transmitted in any form in whole or in part without the prior written permission of Intertek. While due care has been taken during the preparation of this document, Intertek cannot be held responsible for the accuracy of the information herein or for any consequence arising from it. Clients are encouraged to seek Intertek's current advice on their specific needs before acting upon any of the content.