Benefits professionals who are considering recommending mobile health apps for employees need to evaluate the doctors behind them and their security features.
There's a metric ton of mobile health care apps out there, and people keep downloading them like they're going out of style. Experts predict that 500 million smartphone users worldwide will be using a health care app this year, and 50% of the more than 3.4 billion smartphone and tablet users will have downloaded mobile health apps by 2018.¹

That's not actually great news for benefits professionals—A lot of these apps are, quite simply, terrible. The bottom-of-the-barrel apps pose risks of misdiagnoses and incorrect treatments, potentially leaving patients even worse off than before.

The good news? There's a new wave of health apps on the horizon that is trying to help patients, not cash in on the latest trend. These “next-wave apps” can produce improved, potentially lifesaving patient outcomes with the ability to do things like provide access to physicians and offer assistance in emergency medical situations. Others can calculate drug dosage, compile medical records, offer patient education and provide diagnostic support.

How does one tell the difference between the good apps and the bad? There's no shortcut—it's simply a matter of doing due diligence. Employers need to assess the potential threats to patient safety and privacy, weighing the limitations and risks of medical apps against their intended benefits. In doing so, they will be able to determine which apps cut through the hype and really pay off.

Here's what benefits professionals should look for when evaluating mobile apps for their workforce.

Carefully Evaluate the Doctors Behind the App

Think of how heavily we rely on some of the apps on our mobile devices. We rarely question services that make tasks simpler, faster and more efficient. That's fine when making a dinner reservation, checking the weather or looking up driving directions. If the app is unreliable, the worst that can happen is we'll end up on the wrong highway. When a medical app provides information that is inaccurate or unreliable, though, the worst-case scenarios can be life-threatening.

A recent survey by Grand Rounds found that 60% of people know nothing about any of the physicians who treat them and that even fewer know anything about the doctors associated with mobile apps.² Considering this fundamental lack of knowledge about physician quality, it's important that patients don't go blindly into a mobile app that promises to connect them with a doctor. Rather, patients should have access to resources that allow them to effectively research the physician's background, credentials and reviews. And by resources, I don't mean a consumer site like Yelp, which has recommendations and reviews that can't fully be trusted. Nor do I mean they should simply Google the doctor, which again can lead patients down a blind alley.

Rather, patients need to make sure that the physicians treating them are those who best fit their needs in all aspects, ranging from disease specialty to treatment style. Patients need to make sure that those doctors represent the upper tier of specialists in the country and are truly qualified to treat whatever specific condition they may have. In short, the
quality of the physicians behind the app needs to be known.

**Recognize That One Size Doesn’t Fit All**

Not every app is equipped to deal with the needs of each employee. Trying to roll out those apps with a one-size-fits-all approach may actually reduce overall health benefit.

An example of this is Apple’s Health app rollout last October. The Health app made waves when it was first announced and, with the popularity of the iPhone, it was sure to reach millions of people across the globe. But unfortunately for Apple and Apple users, the app was not compatible with standard measures used in the United Kingdom and Australia. Apple had to pull the app so that it could fix the issue. Users who depended on the app to monitor their glucose levels, for example, have had to seek out new tracking systems while they await the fix.

How to avoid this? Benefits professionals can look at their own workforce and evaluate what kind of medical conditions need to be addressed. Maybe the workforce has an unusually high degree of cancer or sports injuries or need for pediatricians. Or maybe new hires are simply confused when they join the company and need help locating a primary care physician within the company’s standard medical networks. Knowing the challenges that employees face will lead to insights about the potential problems that a mobile app can help solve.

**Focus on Dr. Right, Not Dr. Right Now**

People love apps because they’re easy to use and fast. But dangers abound when we prioritize the on-demand ability of mobile health over finding the right doctor, and this temptation needs to be top of mind during the evaluation process.

According to a recent study in *BMJ Quality & Safety*, approximately 12 million, or one in 20, adult outpatients are misdiagnosed in the United States each year. Perhaps even more alarming, in a recent survey conducted by Grand Rounds, 88% of respondents said they either have experienced or know someone who has experienced a severe misdiagnosis, botched surgery or altogether unnecessary surgery due to misdiagnosis. In addition, 17% of those respondents know someone who has died as a result. If this is happening at an individual level during in-person visits, what might the number be for diagnoses reached via consultation over a mobile app?

Recommending such apps could mean a liability for employers if such an incident occurred and, considering the numbers above, it’s a significant risk. When evaluating mobile apps for employees, benefits professionals should not become too enamored with speed and convenience—and instead should keep a tight focus on ensuring that the app can meet an extraordinarily high quality standard.

**Privacy and Security Concerns**

Finally, security may be an issue. As mobile use continues to grow, increasingly sensitive data finds its way onto handheld devices. The October 2014 *California Data Breach Report* revealed the health care sector to be second only to retail in data security breaches and identified lack of proper encryption and lost or stolen hardware as the two main causes of these com-
promises in security. In 2013, the Identity Theft Resource Center showed that health care data accounted for 43% of major breaches, and a 2014 Bitglass report showed loss or theft of employee mobile devices to be the source of 68% of all health care breaches since 2010.

This information is not lost on users. The Grand Rounds 2014 mobile health survey shows that 70% of people reported concern about the privacy and security of mobile health apps. And most apps do a poor job of securing health care information about the patient. An analysis of data practices and privacy risks of several popular mobile health and fitness apps conducted last year by Privacy Rights Clearinghouse revealed that most data on mobile health apps remains unencrypted and that personal information ranging from e-mail addresses to dates of birth may be exposed as data is transferred. The same study showed that most free and paid health apps share the unencrypted data with advertisers and third-party analytics firms.4

Although most mobile health app developers have a passing familiarity with the Health Insurance Portability and Accountability Act (HIPAA), many do not really understand its impact on their apps, which translates into apps that have unclear privacy policies. Being a great coder doesn’t mean being an expert at translating that code into rock-solid HIPAA and protected health information (PHI) compliance. PHI could make its way to a given app in a vulnerable way and become compromised.

The Right Apps—With the Right Doctor—Can Still Help

Despite these concerns, the use of mobile health apps can be a tremendous advantage for benefits professionals. Having the right app in the hands of employees can help them access quality medical care faster as well as help remove the waste from an employer’s health care spending. And mobile apps can even encourage employees to seek out care in the first place at a critical moment in the health care cycle.

Furthermore, as mobile health continues to evolve and mature as an industry, we are likely to see new regulations to help assess, mitigate and manage risks. And there’s nothing wrong with a little regulation if it’s helping screen out the bad apples—or apps, as the case may be. Still, until that time, it’s the responsibility of the employer to determine the risks and benefits of any and all health care apps recommended in the workplace.

For now, the best health apps are ones that are developed jointly by medical and mobile technology experts and that deliver services that consider an employee’s individual health needs. I don’t mean virtual doctors who diagnose or recommend treatment based on symptoms inputted into an app by a would-be patient. Rather, the best apps will be ones that can be relied upon to help connect patients with high-quality medical professionals who can deliver expert advice, proper treatment and positive outcomes for that patient’s highly individual health condition. The best apps would pay attention to all relevant security protocols, including HIPAA as well as a deep adherence to protecting PHI.

An app that can do all this will be well-received by employees. And it won’t cause benefits professionals to lose sleep.

Endnotes


Owen Tripp is co-founder and CEO of Grand Rounds, a company that connects patients to medical experts for second opinions. Tripp previously co-founded Reputation.com, which the World Economic Forum designated as a 2011 Technology Pioneer. He also held leadership positions at eBay and Accenture (Health and Life Sciences Practice). Tripp received a B.A. degree from Trinity College and an M.B.A. degree from Stanford Graduate School of Business.