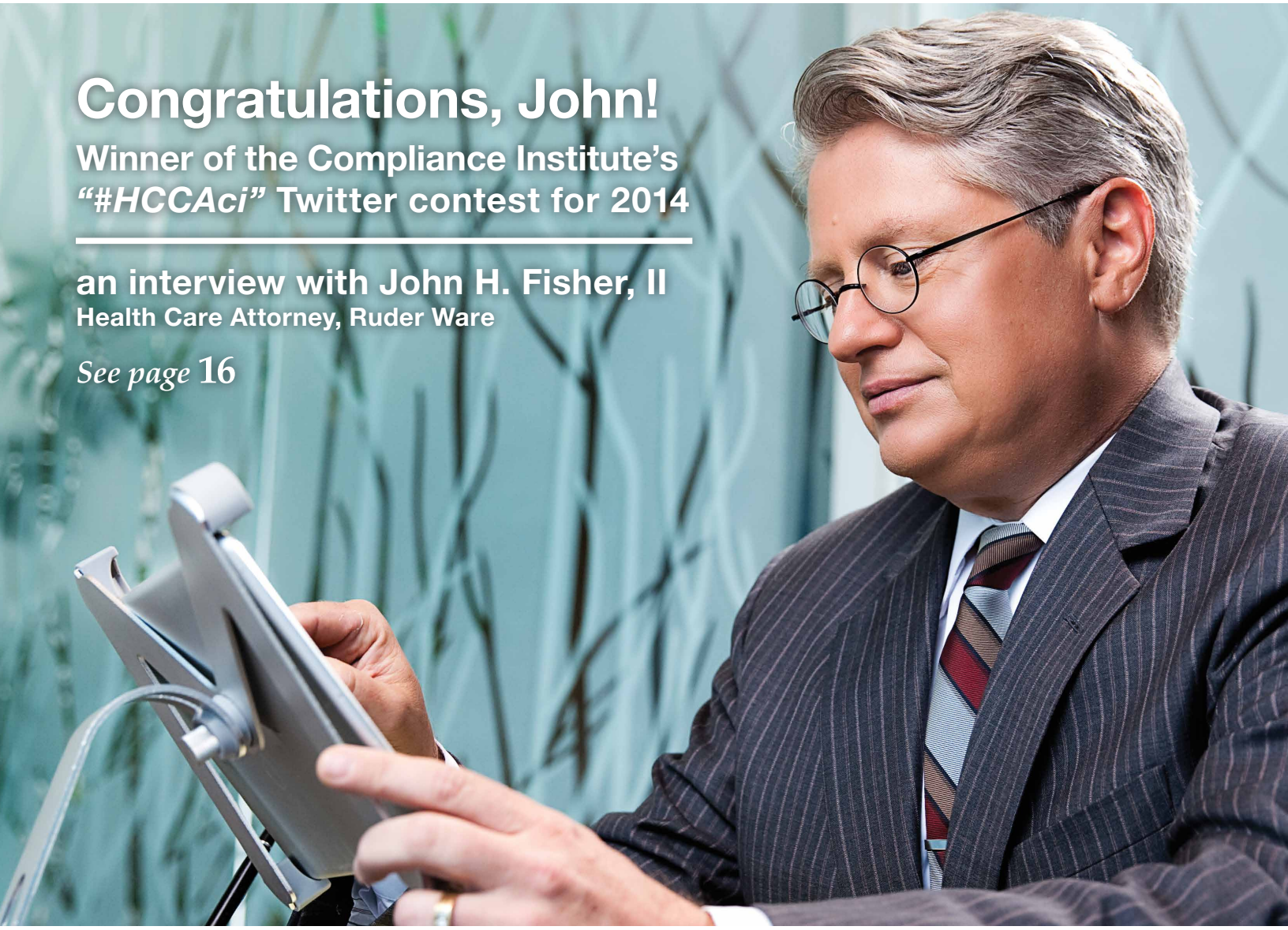
HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

Compliance TODAY

August 2014

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

WWW.HCCA-INFO.ORG



Congratulations, John!

Winner of the Compliance Institute's *"#HCCAci"* Twitter contest for 2014

an interview with John H. Fisher, II

Health Care Attorney, Ruder Ware

See page 16

by Theresamarie Mantese and John R. Wright

Mobile devices and medical apps in the healthcare workplace

» There is a growing multi-billion dollar market for mobile medical apps and devices.
» The FDA regulates apps that turn mobile devices into traditional medical devices.
» The FDA also regulates apps that control attachments or traditional medical devices.
» Healthcare workers are using apps on personal devices brought into the workplace.
» Strong Bring Your Own Device (BYOD) policies are necessary to maintain compliance.

Theresamarie Mantese *(tmantese@healthlex.com) is an Attorney and Shareholder and* ***John R. Wright*** *(jwright@healthlex.com) is an Associate Attorney with Rogers Mantese & Associates, PC located in Farmington Hills, MI.*

Mobile devices and medical applications (apps) are changing the way healthcare data is gathered, analyzed, stored, and shared. Healthcare practitioners are using smartphones and tablets in order to run a wide variety of medical apps that help them care for patients, while using those same devices away from work to control apps that have nothing to do with medicine. Using smartphones and tablets in their daily lives makes healthcare practitioners increasingly comfortable using those devices in the workplace. However, introducing personal devices and non-medical apps into the healthcare environment where there is sensitive information raises compliance concerns. There are risks of unwanted intrusion into a healthcare organization by a virus embedded in an app's software code or an unwanted release of protected patient information that has been placed on a personal device that is then given away, lost, stolen, or hacked.

In order to reduce the risks of data breaches, compliance officers must understand the variety of medical apps in the marketplace as well as current regulations. Once compliance officers understand how medical apps are utilized in their organizations, they can implement policies designed to reduce the risks presented when allowing employees to bring personal devices into the workplace.

Mantese

Wright

Mobile devices and medical apps

Mobile medical apps are software programs that run on smartphones and tablets and turn these ordinary devices—or accessories that attach to them—into regulated medical devices. There are apps that do not meet this definition, yet still relate to health and medicine, such as those apps targeted to consumers to help track health and fitness activities. These health, wellness, and medical apps are exploding in popularity among consumers seeking to improve their own health, as well as among practitioners seeking to improve the health of their patients. Major players in the technology and Internet industries are making serious moves into the healthcare sector. Apple's recent announcement of its Health app and HealthKit platform, Samsung's development of its S Health app and SAMI platform, reports of Google's Google Fit, and WebMD's announcement of Healthy Target app all

evidence the growing popularity and demand for mobile health-tracking products.

Of course, using mobile technology to track one's health is not an entirely new phenomenon. Mobile health (mHealth) systems existed long before the widespread adoption of smartphones, when Personal Digital Assistants (PDAs) gained popularity in the early 1990s.[1] There are arguably even earlier examples of modern mHealth, but the very recent impact on the market for healthcare services is apparent—and this burgeoning industry continues to grow. In fact, the market for mHealth services is expected to reach $26 billion by 2017.[2]

Of course, using mobile technology to track one's health is not an entirely new phenomenon. Mobile health (mHealth) systems existed long before the widespread adoption of smartphones, when [PDAs] gained popularity in the early 1990s.

The most popular medical apps for healthcare practitioners are those used to look up drug information (e.g., Epocrates and mobilePDR, the Physician's Desk Reference app). These apps present a moderate learning curve and are accessible to most users in the health professions, regardless of their respective experience with mHealth. At the other end of the spectrum, newer medical apps being introduced into the market are becoming increasingly sophisticated. For example, there are apps that can turn a smartphone into an electrocardiograph, like the AliveECG system by AliveCor. There are even ingestible "smartpills," such as the Proteus Digital Health Feedback System, consisting of a swallowed sensor that can communicate with a mobile device via Bluetooth technology. Some, but not all, of the available medical apps are prescribed to patients by healthcare professionals. For instance, BlueStar, an FDA-approved medical app, is only available to Type 2 diabetes patients who receive a code from a pharmacist pursuant to a valid prescription.

There are endless examples of creative uses of advanced mobile technology within medical apps, but a medical app's true utility is gauged by how useful it is in the traditional healthcare setting. Market experts predict technology companies developing products for the healthcare industry will start focusing on creating supportive software for healthcare organizations to allow for the collection of data across a wide variety of apps used by both clinicians and patients to conveniently input data into a patient's Electronic Health Record (EHR).[3] The healthcare sector of the information technology industry is ripe for streamlining due to the existence of so many EHR software products and the proliferation of medical apps. Recent studies suggest that improved interoperability between medical devices, or medical devices and EHRs, could save the healthcare industry more than $30 billion per year.[4] Compliance officers are already dealing with EHR headaches, which might make discussion about the even more complex medical app market daunting. Yet, compliance officers should remain cognizant of the fact that once EHR software is integrated with a medical app, then it will fall under the regulatory authority of the Food and Drug Administration (FDA).[5]

FDA regulations

On September 23, 2013, the FDA issued long-awaited final guidance on the regulation of medical apps.[6] As medical apps began to come to market, it became clear that they implicated issues that normally fall under the purview of multiple federal agencies that normally regulate medical device safety and the communications industries. In response, Congress passed the Food and Drug Administration Safety Innovation Act (FDASIA) in 2012, charging the FDA, along with the Office of the National Coordinator for Health Information Technology (ONC) and the Federal Communications Commission (FCC), to issue final recommendations on the regulation of health information technology (Health IT). The recommendations come from the FDASIA Workgroup, a group of experts and stakeholders from various industries appointed to give guidance on a broad range of Health IT issues including mHealth. The FDA expedited its final guidance specifically addressing medical apps after an initial FDASIA Workgroup report recommended the FDA do so.

The FDA guidance on mobile medical apps targets app developers, not companies that make smartphones and tablets, or those that host app stores, such as the Apple App Store and Google Play. Further, the FDA guidance is also not intended to regulate practitioners, unless those practitioners are engaged in a clinical trial with an app as an investigational new medical device. The FDA only intends to regulate apps that pose a risk to a patient's health if used improperly and not apps that pose little or no risk to patient safety.

The FDA regulates apps based on their intended use as advertised by the developers. In its guidance, the FDA uses the example of an app that turns a smartphone into a flashlight by using the smartphone's camera flash. These flashlight apps are most often not intended for use by a health practitioner, nor are they advertised for such purposes. Even though these types of apps could, hypothetically, be used in the healthcare setting to shine a light on a patient during an examination, it is not necessary for the FDA to regulate them. On the other hand, there are apps like iExaminer, a combination of an app and an attachable device, that turn a smartphone into ophthalmoscope by utilizing the flash, camera, and screen on a smartphone. Surely, this type of device could function as a flashlight, but it is designed and advertised for medical use and clearly falls under FDA regulation.

It is important to note that the new FDA guidance does not create any new rules or regulations. Rather, the guidance is intended to show how the FDA will apply current rules and regulations designed to regulate traditional medical devices. Presently, medical devices are separated into three regulatory classes: Class I has the least amount of regulation, Class II has more, and Class III has the most.[7] The FDA is focused on regulating medical apps that transform a mobile device into what would be considered a traditional medical device, as well as medical apps that control traditional medical devices. For those apps that do not meet these criteria, the FDA

The FDA only intends to regulate apps that pose a risk to a patient's health if used improperly and not apps that pose little or no risk to patient safety.

maintains what it calls "enforcement discretion," meaning it will not regulate the app but reserves the authority to decide to in the future. On the FDA's website, there are separate pages listing examples of apps that fall into each of the three classes, as well as a list of apps that are examples of what the FDA does not regulate.

More recently, in its final recommendations published in a report on April 3, 2014, the FDASIA Workgroup confirmed the scope of the FDA's regulation of medical apps expressed in the new FDA guidance and recommended against any further expansion.[8] The report confirms that the FDA will continue to exercise its regulatory authority over medical apps. However, keep in mind that the current regulatory landscape is always subject to congressional action. Congress could enact legislation in the future that alters the FDA's authority to regulate medical apps. Certain developments on Capitol Hill suggest that some kind of congressional intervention is likely. The House of Representatives is currently considering the Sensible Oversight for Technology which Advances Regulatory Efficiency (SOFTWARE) Act of 2014, and the Senate is considering the Preventing Regulatory Overreach To Enhance Care Technology (PROTECT) Act of 2014. Both of these acts seek to limit the FDA's authority to regulate apps, under the premise of creating a more favorable environment for smaller innovators who will have a harder time clearing regulatory hurdles. To further accomplish this stated goal, on March 18, 2014, a bipartisan group of U.S. Senators sent the FDA a letter regarding medical apps, requesting more information on how the FDA intends to proceed with its regulations. All of this is to say that the regulatory environment for medical apps has yet to be resolved by the federal government and is definitely an area that should be monitored by compliance officers.

mHealth in the healthcare workplace

Compliance officers should not only be aware of the apps that are available to clinicians in the healthcare setting, but also be aware of how they operate and on what devices. Compliance officers should also recognize that many medical apps are hosted on personal devices that belong to the healthcare practitioner and are not owned or controlled by the practitioner's employer. Employees may opt to use their own personal devices in the workplace, even if an employer supplies a smartphone or a tablet to an employee for work use.

This raises an issue for compliance officers as to whether to implement a Bring Your Own Device (BYOD) policy. It is advisable that compliance officers focus on the development of BYOD policies before any catastrophic security breach occurs. Even if an organization bans the use of personal devices on the organization's network, an employee still has the potential to share information over a cellular data network, a Bluetooth connection, or by manually uploading information to a device.

Banning personal devices may be impractical, if not impossible, and there may be good reason to encourage use of personal devices. There is some evidence to suggest that allowing healthcare employees to bring their own devices to work increases productivity and makes workers happier.[9]

Even if an organization bans the use of personal devices… an employee still has the potential to share information over a cellular data network, a Bluetooth connection, or by manually uploading information to a device.

Compliance officers should educate employees on the risks of using a personal device at work and establish a clear BYOD policy. One of the easiest policies to implement in order to protect the dissemination of sensitive information via personal devices is requiring users to "lock" and enable the password-protection function on their devices. This is not a fail-safe method of protecting information within the device itself, but it is one small step in the right direction. Unfortunately, according to one survey, only 59% of people working in the healthcare industry who used their own smartphone at work enabled the password-protection function.[10] That remaining 41% presents a significant security risk.

Other policies are more difficult to implement and present additional challenges. For instance, some BYOD policies call for the ability of the employer to remotely wipe out all of the data on the device. However, an employee may be hesitant to allow an employer access to his/her private data and the ability to see and destroy it. As with any compliance program, a policy is no good unless users are willing to abide by it. Employees may be reluctant to abide by an overly-restrictive BYOD policy.

Even though an employee might share all sorts of personal information on the Internet, allowing advertisers to track and locate

travel and shopping habits, an employee may nevertheless object to a policy that requires tracking software on his/her mobile device while at work. In fairness, if an organization is collecting data about employees through the use of technology in the workplace, employees should understand the scope of that intrusion and its justification. A market-based solution to this problem that is gaining momentum among companies and employees alike is the development of "dual-identity" devices that contain two separate operating systems—one for personal use and one for business. This allows for a certain amount of control by the employer while maintaining employee privacy.

Compliance officers should consider surveying employees on whether they use smartphones or other devices in the workplace. More specifically, employees should be asked about the particular apps they use and how they use them. If clinicians are sending text messages to each other, are they being sent via an app over a secure Wi-Fi network, a public network, or a cellular data network? Are the messages being stored in an inbox with all of the recipient's personal messages? Or, are the messages stored in a regulated, stand-alone app that is marketed to health professionals and encrypted to be compliant with state and federal privacy laws?

If text messaging is popular among employees, then a compliance officer may consider exploring the purchase of an app for employees to use for secure messaging with the ability to remotely wipe the app and all of its contents from the employee's personal device, leaving the rest of the employee's device intact. Apps can also be custom designed for internal use within an organization by employees only and controlled by the employer's IT department. This is perhaps the best way to control who is using a medical app and how the medical app is being used by the employees.

Conclusion

There is no one-size-fits-all BYOD policy. Compliance officers should work with IT professionals to understand their organization's communications infrastructure and determine how best to allocate resources. Of course, BYOD policies will cover non-IT topics too, such as sanitation of smartphones. These devices are notorious for harboring germs, but who should be responsible for cleaning them? The costs saved by allowing employees to bring their own devices rather than using smartphones and tablets issued by an employer are significant, but could be outweighed by losses resulting from a data breach or loss of proprietary information. Understanding the risk of non-compliance, an organization might consider "cyber liability" insurance coverage in case of data breach or a cyberattack. As the mHealth market continues to develop, it will be important to stay current on the growing number of mobile medical apps and their regulation as medical devices by the FDA as well as proposed federal legislation. With a firm grasp on the technology, compliance officers can develop BYOD policies that enhance healthcare workers' abilities and protect patient safety and privacy.

1. Alex Krouse: "iPads, iPhones, Androids, and Smartphones: FDA Regulation of Mobile Phone Applications As Medical Devices." *Independent Health Law Review*, 2012: vol 9, pp 731, 733
2. Diane Cooper: "Understanding the Impact of the FDA Guidance for Mobile Medical Applications: Is There an App for That?" Quinnipiac Law Review, 2013: vol 32, pp 95, 113
3. Mark McAndrew: "In Apple's Healthcare Play, Will BYOD = Bring Your Own Data?" *Managed Market Access*, February 22, 2014. Available at: http://bit.ly/1tjyY83
4. West Health Institute: "The Value of Medical Device Interoperability: Improving patient care with more than $30 billion in annual healthcare savings." March 2013. Available at http://bit.ly/XXXXXXX
5. Paul DeMuro and Nick Healey: "Emerging Healthcare Information Technologies and the Legal Challenges They Present." *Wyoming Lawyer*, October 2013, pp 24, 26.
6. Food and Drug Administration, press release: "FDA issues final guidance on mobile medical apps." September 23, 2013. Available at http://1.usa.gov/1pXdGLX; PDF form available at: http://1.usa.gov/1pXdSuL
7. 21 U.S.C. Code § 360c: "Classification of devises intended for human use." 2014. Available at http://bit.ly/1r63ihW; *See also* FDA Website at: http://1.usa.gov/U1gVDn
8. FDASIA Health IT Report: Proposed Strategy and Recommendations for a Risk-Based Framework. April 2014. Available at http://1.usa.gov/1zmSWiv
9. The White House/Digital Government: *Bring Your Own Device, A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs.* August 23, 2012. Available at http://1.usa.gov/TQnisU
10. Cisco mConcierge website: BYOD Insights 2013, A Cisco partner network study. Available at http://bit.ly/1r644M2