Where's the App for That?
Mobile Medical Apps, Cybersecurity and the Regulatory and Litigation Landscape

---

Sharon R. Klein
Pepper Hamilton LLP
Los Angeles

Jan P. Levine
Pepper Hamilton LLP
Philadelphia

Angelo A. Stio III
Pepper Hamilton LLP
Princeton

T. Stephen Jenkins
Pepper Hamilton LLP
Philadelphia

Alex C. Nisenbaum
Pepper Hamilton LLP
Los Angeles

TABLE OF CONTENTS

I. The Federal Trade Commission's Authority and Enforcement Actions

A. Traditional Regulation of Privacy Under Section 5

Historically, the Federal Trade Commission (FTC) has been the most active federal regulator of data privacy and security. Although created in 1914, the FTC first began policing data privacy and security in 1995. Since that time, the FTC has pursued hundreds of cases against companies that have violated privacy statutes or engaged in unfair or deceptive practices that put consumers' personal identifying information at unreasonable risk. In this regard, the FTC has asserted seemingly unbridled authority to protect consumer privacy and ensure data security.

The FTC's general enforcement authority is derived from Section 5 of the Federal Trade Commission Act (FTC Act). Section 5 of the FTC Act (15 U.S.C. § 45) prohibits "unfair or deceptive acts or practices in or affecting commerce." This section has been interpreted as conferring the FTC with jurisdiction to police deceptive acts (the Deception Prong) or unfair practices (the Unfairness Prong).

Actions pursued under the Deception Prong typically involve a company's failure to adhere to express or implied claims it makes about security it will provide. More recently, the FTC has regulated privacy under the Unfairness Prong. The FTC has interpreted "unfair" to mean something more akin to deviating from industry standards or minimal protections, at least in the privacy and data security sector. The FTC's recent litigation with Wyndham Worldwide discusses, in depth, the FTC's broad authority to regulate privacy and security.

In *FTC v. Wyndham Worldwide Corp.*, the FTC sued Wyndham following multiple data breaches that affected various entities in the Wyndham Worldwide Corporation family of companies (Wyndham Companies) from 2008 to 2009.[1] Based on those breaches, the FTC alleged that the defendants failed to have "reasonable and appropriate" cybersecurity practices.[2] The FTC cited the following deficiencies in support of its claims: inadequate firewalls; unencrypted storage of credit card information; inadequate information security policies and procedures; outdated operating systems; use of default user IDs and passwords; user IDs and passwords of insufficient complexity; inadequate methods of inventorying computers connected to the network; lack of reasonable measures to detect, prevent and investigate unauthorized network access; failure to properly follow incident report procedures; and inadequate restriction on third-party vendors' access to the network.[3]

Relying on these allegations, the FTC's complaint had two counts. First, the FTC claimed that Wyndham engaged in *deceptive* practices under Section 5(a) for the Act (15 U.S.C. § 45(a)) by failing to fulfill the representations it made to its customers about the data security

---

[1] *See* First Amended Complaint for Injunctive & Other Equitable Relief ¶¶ 7-11, 26-40, *FTC v. Wyndham Worldwide Corp.*, No. 2:13-cv-01887-ES-JAD (D.N.J.) (filed Aug. 9, 2012).

[2] *See id.* at ¶¶ 44, 47.

[3] *See id.* at ¶¶ 24(a)-(j).

practices in place to protect customers' personal information (the Deception Claim).[4] Second, the FTC claimed that the Wyndham Companies also engaged in *unfair* practices under Section 5(a) by failing to employ "reasonable and appropriate measures to protect personal information against unauthorized access" (the Unfairness Claim).[5]

Wyndham Hotel & Resorts (Wyndham), one of the Wyndham Companies, filed a motion to dismiss both counts of the FTC's complaint. Regarding the Unfairness Claim, Wyndham challenged the FTC's authority to regulate cybersecurity, the adequacy of the FTC's notice about "reasonable and appropriate" cybersecurity, and the sufficiency of the FTC's pleading.[6] The district court ultimately denied Wyndham's motion and found that the FTC Act permitted the FTC to regulate cybersecurity practices.[7] In so doing, the court refused "to carve out a data-security exception to the FTC's unfairness authority" and concluded that "fair notice" does not "require[] the FTC to formally issue rules and regulations before it can file an unfairness claim in federal district court."[8] Recognizing the evolving landscape of cybersecurity, the court further explained that the prohibitions in Section 5 of the FTC Act are "necessarily flexible" and intended for "cases arising out of unprecedented situations."[9] According to the court, the FTC's complaints, consent agreements, public statements and business guidance brochure provide sufficient guidance to companies about the FTC's standards for reasonable data security practices.[10]

In affirming the district court's decision, the U.S. Court of Appeals for the Third Circuit addressed the meaning of "unfair" under the FTC Act. The court explained that unfair practices (1) require substantial injury to customers (2) that is not reasonably avoided by consumers and (3) is not outweighed by benefits to consumers or to competition.[11] In considering these requirements, the court concluded:

- An unfair practices claim under the Act does not require "unscrupulous or unethical" behavior.
- A company is not insulated from an FTC action under the FTC Act merely because the company was the victim of a crime.

---

[4] *See id.* at ¶¶ 44-46.

[5] *See id.* at ¶¶ 47-49.

[6] *FTC v. Wyndham Worldwide Corp*., 10 F. Supp. 3d 602, 607 (D.N.J. 2014), *aff'd by* 799 F.3d 236 (3d Cir. 2015).

[7] *Id.* at 612-15.

[8] *Id.* at 612, 617.

[9] *Id.*at 619-20.

[10] *Id.* at 620.

[11] *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236, 244 (3d Cir. 2015).

- Wyndham's privacy policy could implicate the "reasonably avoided" requirement of an unfairness claim, while also serving as the basis for a "deception" claim under the FTC Act.[12]

After *Wyndham*, there is no doubt that the FTC has authority to regulate privacy and data security under Section 5. In the area of mobile *medical* applications and devices, companies should expect the FTC to stretch its regulatory legs. As of the date of this publication, there have been no significant FTC enforcement actions or adjudications regarding mobile medical applications and devices. But the FTC has long regulated mobile applications and devices, and the same principles that apply to mobile applications and devices are undoubtedly applicable to the medical industry. Some of these principles include encouraging companies to design products with privacy in mind (Privacy by Design), to embed security into every step of the product development and implementation (Start with Security), and to be aware of the increasing number of Internet-connected devices (Internet of Things).

II. Privacy by Design

The FTC has long cared about the privacy of consumer information. In March 2012, the FTC issued a report titled "Protecting Consumer Privacy in an Era of Rapid Change" (Protecting Consumers Report), which was geared to help businesses and policymakers safeguard consumer privacy.[13] As part of this report, the FTC discussed the concept of privacy by design, or rather the baseline principle that companies should use to promote consumer privacy throughout their organizations and at every stage of the development of their products and services.[14]

In promoting privacy by design, the FTC has encouraged companies to "build in" privacy by default by, for example,

- Putting limitations on data collection and retention
- Deleting consumer data when no longer needed and allowing consumers to do the same
- Maintaining reasonable accuracy of data
- Increasing efforts to educate consumers about the commercial collection and use of their data and the availability of privacy tools

---

[12] *Id.* at 244-46.

[13] FTC, "Protecting Consumer Privacy in an Era of Rapid Change" (March 2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [*hereinafter* Protecting Consumers Report].

[14] *See id.* at 22.

- Designating a person responsible for privacy, training employees and ensuring adequate oversight of third parties

- Providing reasonable security for data

In the context of mobile medical applications and devices, the FTC's guidance is particularly important given the heightened value of health information. The fact that an organization is not covered by the Health Insurance Portability and Accountability Act (HIPAA) does not decrease the risk or threat of breach. Thus, manufacturers and distributors of mobile medical applications and devices must be just as vigilant in building privacy into the design and development of their products.

III. Start with Security

Another way to prevent the dissemination of personal identifying information is to minimize the risk of breach. In June 2015, the FTC provided an overview of more than 50 of its data security enforcement actions in its "Start with Security" guidance.[15] This guidance distilled those more than 50 enforcement actions into 10 principles to consider when attempting to reduce security vulnerabilities:

1. Start with security.

2. Control access to data sensibly.

3. Require secure passwords and authentication.

4. Store sensitive personal information securely and protect it during transmission.

5. Segment your network and monitor who is trying to get in and out.

6. Secure remote access to your network.

7. Apply sound security practices when developing new products.

8. Make sure your service providers implement reasonable security standards.

9. Put procedures in place to keep your security current and address vulnerabilities that may arise.

10. Secure paper, physical media and devices.

We discuss below how each step applies to businesses, in general, and to mobile medical applications and devices, specifically.

[15] FTC, "Start with Security: A Guide for Business" (June 2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

A. Step One: Start With Security

Similar to privacy by design, as a company, you should factor security into decision-making in every part of your business — personnel, sales, accounting, information technology, etc. Make conscious choices that are appropriate for your business about what data to collect, how long to keep the data, and who can access the data.

One of the enforcement actions that the FTC cites for this step is Accretive Health. Accretive Health is a revenue-cycle operations servicer. As part of those services, Accretive collects, maintains and accesses information about hospitals' patients, including sensitive health and personal information. Basically, Accretive Health handles the backend of hospital administration.

Accretive Health used actual live consumer personal information for training purposes. But Accretive Health did not ensure that the information was removed from its employees' computers following training. An employee left a laptop containing information relating to 23,000 patients in a locked passenger compartment of a car, which was then stolen.

There was no reason to use real consumer personal information for training purposes. If you need examples, use "Jane Doe" or "John Smith" or some other fictional name. As it relates to mobile medical applications, only use personally identifiable information (PII) if absolutely necessary. Similar to privacy by design, if there is a way to achieve the same functionality without PII, then PII may not be necessary.

The other two lessons from this enforcement action go hand in hand. Protect devices that process personal information. Keep safety standards in place when data is en route by implementing reasonable security policies. In Accretive Health, a secure server would have been a better option for accessing the data (if the data was needed at all).

For mobile apps and devices, use reasonable security policies for transmitting data that protect the data in all modes of transport. For example, instead of storing data on a mobile device, consider storing data in an encrypted cloud. When transmitting data, use industry standards, like secure socket layer encryption. And make sure your transmission of data is compatible with the devices for which your medical application will be installed. If your app does not function properly, it exposes you and your customers to risk of vulnerability.

Ultimately, starting with security boils down to three "don'ts":

- Don't collect personal information you do not need.
- Don't hold on to information longer than you have a legitimate business need.
- Don't use personal information when it is not necessary

B. Step Two: Control Access to Data Sensibly

If you decide your business has a legitimate need to hold on to sensitive data, take reasonable steps to secure it from both outsiders and employees. Almost 70 percent of breaches occur from the actions of employees or other authorized users. Thus, when deciding who to give

access to, restrict access to only those minimally necessary users, for example, those employees who need access to sensitive data to perform their jobs.

The example the FTC gave in its Start with Security guidance was its enforcement action with Twitter. Twitter collected public information, such as user profiles, and nonpublic information, such as email addresses, IP addresses and mobile phone numbers. Twitter granted almost all of its employees the ability to exercise administrative control of Twitter's systems, including the ability to reset a user's account password, view a user's nonpublic tweets and other nonpublic user information, and send tweets on behalf of a user. This increased the risk that compromise of an employee's credentials could cause a serious breach.

In the context of mobile medical applications and devices, be careful who has administrative access to applications and devices. Most employees do not need administrative access to perform their job functions. Thus you should,

- Restrict access to sensitive data.
- Limit administrative access.

C. Step Three: Require Secure Passwords and Authentication

Strong authentication procedures can help ensure that only authorized individuals have access to sensitive data. Similar to step two, having secure passwords and authentication restricts unauthorized access to data.

Again, the Twitter enforcement action is instructive on this point. In that action, the FTC alleged that Twitter did not establish or enforce policies that prohibited the use of common dictionary words as administrative passwords. Twitter also did not establish or enforce policies that required administrative passwords to be different from any password an employee used to access third-party websites and services. Twitter failed to prohibit storage of administrative passwords in plain text in personal email accounts. And Twitter did not suspend or disable administrative passwords after a reasonable number of unsuccessful log-in attempts.

Were a mobile medical application or device manufacturer to take Twitter's approach, they could potentially put their users at an even greater risk. To take an example from pop culture, consider the television series "Homeland" and the remote hacking of fictional character Vice President Walden's pacemaker. Because the hacker was able to trick or otherwise bypass authentication procedures, the hacker was able to induce a heart attack, killing Vice President Walden.

Despite the fictional nature of this example, along with the FTC's guidance, it teaches the following lessons:

- Insist on complex and unique passwords.
- Store passwords securely.
- Guard against brute force attacks.

- Protect against authentication bypass.

D. Step Four: Store Sensitive Personal Information Securely and Protect It During Transmission

It is not enough to protect against brute force attacks at an endpoint location; data must be protected throughout every step of the process, including during transmission. One of the methods to protect personal information during transmission is through encryption. Encryption is the process of encoding messages or information in such a way that only an authorized party can read it. Employing encryption architecture is a recognized best practice.

An example of the pitfalls of not protecting confidential information in transmission comes from the FTC's enforcement action against Fandango. There, Fandango provided a website and an iOS mobile application that allowed consumers to purchase movie tickets and view show times, trailers, and reviews remotely. Online services, such as the services offered by Fandango, often use the Secure Sockets Layer (SSL) protocol to establish authentic, encrypted connections. SSL relies on electronic documents called SSL certificates to properly authenticate and encrypt. If an application does not perform SSL certificate validation, it can allow an unauthorized third party to provide a fake certificate and decrypt, monitor or alter communications (a "man-in-the-middle" attack).

The iOS operating system application programming interfaces used by app developers validate SSL certificates by default. The iOS developer documentation warns developers like Fandango against disabling the default setting or otherwise failing to validate SSL certificates. Apparently, Fandango overrode the iOS default and turned off the SSL certificate validation process. It did not implement any security measures that compensated for the lack of SSL certificate validation.

In the Fandango action, failing to ensure proper security measures may have exposed millions of users' sensitive information. The same risks exist in the context of mobile medical applications and devices. Often, the harm is greater given the value of health-related information. Distributors of mobile medical applications and devices should do the following:

- Keep sensitive information secure throughout its life cycle.

- Use industry-tested and accepted methods.

- Ensure proper configuration.

E. Step Five: Segment in Your Network and Monitor Who Is Trying to Get In and Out

Appropriately segment networks and use intrusion detection and prevention tools to monitor for malicious activity. This principle is two-fold: Not every segment of a network needs heightened security or encryption (*e.g.*, a public-facing website). For those network areas that contain sensitive information, however, special attention should be given to who has access.

The FTC used an enforcement action against Dave & Buster's to demonstrate this principle. Dave & Buster's operates a chain of restaurants around the United States and operates computer networks in each store as well as a corporate computer network. The networks link corporate headquarters with each store. As part of its restaurant operations, Dave & Buster's collected payment card information and transmitted it from its in-store network to a third-party credit card processing company.

The FTC alleged that Dave & Buster's engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its networks. For example, Dave & Buster's did not use a security detection system or monitor system logs, nor did Dave & Buster's monitor and filter outbound traffic from its networks to identify and block export of personal information without authorization. Additionally, Dave & Buster's failed to adequately limit access between in-store networks, such as by using firewalls or isolating the payment card system. Consequently, an intruder was able to gain unauthorized access to the Dave & Buster's network and intercept personal information in transit from its store networks to its credit card processing company.

To prevent intruders from gaining access to sensitive health-related information, distributors of mobile medical applications and devices should be vigilant in monitoring who has accessed their networks. Segmenting public-facing websites or network segments with little to no PII from network segments with sensitive information could aid in lowering security risks.

F. Step Six: Secure Remote Access to Your Network

If employees, clients or service providers are given remote access to a company's network, make sure steps to secure those access points are taken. Remote access, while helpful, can expose a network to numerous risks if security measures are not taken. Providing unnecessary levels of access to third-party vendors can expose consumers to unreasonable risks.

As many are familiar, the Target data breach is a prime example of why security by design is a helpful endeavor. Hackers were able to upload malware onto Target's point of sale (POS) systems by using credentials stolen from a Target HVAC vendor. The HVAC vendor had access rights to Target's network to conduct tasks like monitor energy consumption and temperatures. The vendor had no need to access Target's POS system to perform these tasks. However, the components of the Target network that the vendor was able to access through its credentials were not properly segmented from its POS systems, allowing hackers to access sensitive payment card information. Hackers stole data on about 40 million credit and debit cards.

From a mobile medical applications and devices standpoint, be mindful of what level of access you provide to employees, clients and service providers. For example, it may be beneficial for health care providers to have access to a health care system's network, especially if the provider is providing at-home or concierge treatment. Be mindful that devices in physical transit are more likely to be lost or stolen. To the extent remote access is given,

- Ensure endpoint security.

- Put sensible access limits in place.

G. Step Seven: Apply Sound Security Practices When Developing New Products

When developing new products and services, ensure that the product or service is designed so that sensitive data transmitted or stored when using the product is secure. This principle is the sister principle to privacy by design. If products are designed with security in mind, risk of harm to the consumer is lowered.

To demonstrate this principle, the FTC examined its enforcement against TRENDnet, a seller of networking devices, such as routers, modems, security cameras and baby monitors that allow users to conduct remote surveillance of their homes and businesses via the Internet. TRENDnet's cameras were by default set to require the input of user credentials prior to viewing the cameras. TRENDnet provided an option that allowed users to make a camera feed publicly available and not require credentials for access. The software did not honor a user's selection to keep the camera feed private. As a result, all users' live feeds were publicly accessible, regardless of the choice reflected in the software's user interface. Hackers discovered the vulnerability and made it public. Links to the feeds of more than 700 cameras were posted online, showing sleeping infants, children playing and other private household activities.

Regarding mobile medical applications and devices, be careful to build security into the product design. Make sure the product performs the way it was designed to perform. Traditional manufacturers have long audited and monitored production for product defects. Do the same thing for your mobile medical apps and devices. Some best practices are:

- Ensure the use of secure coding.
- Follow platform guidelines for security.
- Verify that privacy and security features work.
- Test for common vulnerabilities.

H. Step Eight: Make Sure Service Providers Implement Reasonable Security Measures

No business is an island. Ensure that service providers implement appropriate security measures for personal information. The FTC's enforcement action against GMR Transcription Services is instructive on this principle. GMR provided services to transcribe audio files, including for health care providers and hospitals, that included sensitive information about consumers. GMR represented in its privacy policy and in other statements that its services were secure and that it was HIPAA compliant. GMR relied almost exclusively on third-party service providers to transcribe the audio files, including medical transcription files, and used third-party service providers to provide IT services for its computer network and online presence.

The FTC alleged that GMR did not adequately verify that its major service provider for medical transcription implemented reasonable security measures. First, GMR did not require by contract that its service provider adopt and implement appropriate security

measures, such as storing and transmitting files securely or requiring authentication of users before granting access to files. Second, GMR did not request or review information about its service provider's security practices, such as the service provider's written information about its security program or audits or assessments of its computer network.

If you engage a third party to develop an application or sign up for a third-party platform, vet the application or platform, perform audits and monitor the vendor. Ultimately, you could be held responsible for the actions of your third-party vendors. To summarize, you should:

- Put it in writing when contracting with third-party vendors.
- Verify compliance through audits.

I. Step Nine: Put Procedures in Place to Keep Security Current and Address Vulnerabilities That May Arise

Security is an ongoing process, not a one-time project. Creating a security protocol and putting reasonable security measures in place is just the first step. Security protections must be updated as the threats to security evolve and as new processes are implemented into product design or services rendered.

The FTC discussed addressing vulnerabilities to security with reference to the TJX enforcement action. TJX is an off-price retailer selling apparel and home fashions through the T.J. Maxx, Marshalls and other brands. TJX routinely used its computer networks to collect personal information from consumers to obtain authorization for payment card purchases, verify personal checks and process merchandise returned without receipts.

The FTC alleged that many of TJX's practices failed to provide reasonable and appropriate security. For example, TJX used insufficient measures to detect and prevent unauthorized access to computer networks, such as by patching or updating anti-virus software. Additionally, TJX was alleged to have failed to follow up on security warnings and intrusion alerts.

Although TJX is a merchant, developers of mobile medical applications and devices face the similar security vulnerabilities. However, the risk to victims of security breaches for medical applications and devices could be life threatening. From the TJX enforcement action, the following lessons should be heeded:

- Update and patch third-party software.
- Heed credible security warnings, and move quickly to fix them.

J. Step Ten: Secure Paper, Physical Media and Devices

Do not forget about paperwork and physical media. In an age of increased dependency on electronic communication, paper is often long forgotten as a vector for PII. But purchase orders, patient forms and other routine paper processes contain PII, and holders of this information must be careful to secure their proper destruction. Additionally, physical media and

devices are often discarded without consideration of the PII or other sensitive information they may contain.

The FTC enforcement action against Gregory Navone is an example of improper destruction of paper files and physical media. Gregory Navone owned and operated businesses that included two mortgage companies. Navone stored sensitive consumer information, which included consumer reports and information derived from consumer reports, in boxes in his garage. Navone disposed of documents containing sensitive consumer information by placing them in a publicly accessible dumpster outside of his office building. The FTC alleged that Navone failed to implement reasonable and appropriate measures to protect sensitive consumer information from unauthorized access.

As one can see from the Navone action, as well the Accretive Health action previously discussed, failing to properly dispose of paper, physical media and devices increases the risk of PII exposure. When mobile medical devices or applications are no longer needed, distributors of those devices should secure their proper destruction. To the extent a device has left the purview of control of the distributor, distributors may want to offer consumers the ability to return the device to the distributor for destruction, or, at a minimum, the distributor should make the consumer aware of the risk of improper destruction. When destroying paper, physical media and devices:

- Securely store sensitive files.
- Protect devices that process personal information.
- Keep safety standards in place when data is en route.
- Dispose of sensitive data securely.

IV. Internet of Things

The Internet of Things is shorthand for the network of physical objects embedded with electronics and software that enable these objects to collect and exchange data. As time goes on, more and more people are using connected devices, such as cell phones, watches or even pacemakers. And, as we learned from "Homeland," these devices are susceptible to hacking.

In January 2015, the FTC issued a report aptly titled "Internet of Things," (IoT Report).[16] This report was partially the result of a workshop titled "The Internet of Things: Privacy and Security in a Connected World," which took place on November 19, 2013.[17] The

[16] FTC, "Internet of Things" (Jan. 2015), *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [*hereinafter* IoT Report].

[17] *Id.* at 3.

workshop featured several panels focused on different aspects of the Internet of Things, including "Connected Health and Fitness."

After the workshop, the FTC laid out in the IoT Report the benefits and risks associated with the Internet of Things, as well as an application of traditional privacy principles to the Internet of Things.

A. Benefits and Risks

The IoT report explicitly acknowledged that the Internet of Things is beneficial to the health care community, stating:

> One area in which these benefits appear highly promising is health care. For example, insulin pumps and blood-pressure cuffs that connect to a mobile app can enable people to record, track, and monitor their own vital signs, without having to go to a doctor's office. This is especially beneficial for aging patients, for whom connected health devices can provide treatment options that would allow them to manage their health care at home without the need for long-term hospital stays or transition to a long-term care facility.[18]

Internet-connected devices allow for patients to be active in their own treatment and allow health care providers to moderate treatment more swiftly. For example, an FTC workshop "participant described a clinical trial showing that, when diabetic patients used connected glucose monitors, and their physicians received that data, those physicians were five times more likely to adjust medications, resulting in better disease management and substantial financial savings for patients."[19]

Nevertheless, Internet-connected devices are inherent with many risks. For example, the FTC noted that IoT devices may be subject to both privacy risks (*e.g.*, collection of sensitive information, such as precise geolocation; collection of habits, locations and physical conditions over time; and use of data to make credit, insurance and employment decisions) and security risks (*e.g.* unauthorized access, facilitating attacks on other systems and other safety risks).[20]

Although the IoT Report applied a number of traditional privacy principles to Internet-connected devices, the issue that was most striking in terms of mobile medical applications and devices is the concept of notice and choice. The principle of notice and choice gives users of IoT devices warning that their information is being collected and the option to opt out (or opt in).

---

[18] *See id.* at 7 (internal quotation marks omitted).

[19] *See id.*at 8.

[20] *See generally id.* at 10-18.

As the IoT Report points out, many IoT medical devices "have no screen or other interface to communicate with the consumer, thereby making notice on the device itself difficult, if not impossible."[21] And, even if a device has a screen, "IoT sensors may collect data at times when the consumer may not be able to read a notice (for example, while driving)."[22]

In the context of mobile medical applications and devices, health care providers are already primed to offer notice and choice, as they are obligated under the doctrine of informed consent to obtain permission before conducting treatment on a patient. To the extent mobile medical applications and devices become a part of the treatment plan of a patient, incorporating notice and choice into the informed consent process could be seamless. However, like any medical procedure or course of treatment, mobile medical applications and devices continue to have certain risks, and the FTC, as well as other regulatory authorities like the Food and Drug Administration (FDA), continue to be concerned with the safety and efficacy of these applications and devices.

V. Overview of FDA Regulation of Medical Devices

Traditionally, the FDA has regulated medical "devices,"[23] such as surgical instruments and stethoscopes. As in every other aspect of our everyday lives, however, software and computer technology were integrated into medical devices to enhance and improve patient care. In the late 1980s, the FDA began publicly suggesting that electronic medical records were within its jurisdiction. Since then, the proliferation of mobile computing platforms and the applications they run, including health care-related mobile applications, has exploded. In addition, thanks to the accessibility of mobile platforms and programming languages, health care organizations may even find that their staff and associated medical professionals are creating new mobile applications or modifying existing mobile applications for use to treat patients in a clinical setting. This creates the potential for health care organizations to be both traditional consumers of mobile applications developed by third parties and developers of mobile applications themselves.

The FDA responded to the increasing number of health care-related mobile applications by issuing final guidance on its regulation of mobile medical applications on September 25, 2013, which was superseded by updated guidance on February 9, 2015 (FDA Guidance).[24] Since the release of the initial version of its mobile medical applications guidance

---

[21] *Id.* at 22.

[22] *Id.*

[23] *See* 21 U.S.C. § 321. The definition provides, in pertinent part, that a "device" is "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory, which is … intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease … or intended to affect the structure or any function of the body."

[24] FDA, "Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff" (Sept. 25, 2013), *available at* http://www.fda.gov/downloads/MedicalDevices/.../UCM263366.pdf [*hereinafter* FDA Guidance].

in 2013, the FDA has approved hundreds of mobile medical applications that focus, generally, on chronic condition management. Additionally, the FDA has shown an increased interest in cybersecurity issues. The FDA released separate guidance for manufacturers of mobile medical applications and other medical devices regarding the management of cybersecurity risks in the design and development of interconnected medical devices on October 2, 2014 (FDA Cybersecurity Guidance).[25]

VI. The FDA View of the Mobile Application Landscape

The FDA Guidance generally provides that, while there are many different kinds of health care-related mobile applications that may be used in a clinical setting or to enhance patient care, only those types of mobile applications the FDA believes present a safety risk to patients will be subject to FDA regulation. Therefore, it is critical that organizations, especially those that may engage in mobile application development, are able to recognize when FDA regulation applies to a mobile application so that they can ensure that applicable FDA regulatory requirements are met. Such requirements may include mandatory registration of entities that manufacture mobile medical applications and their mobile medical applications, adherence to good manufacturing practices, premarket notification to the FDA, and adverse incident reporting, among other requirements.

The FDA Guidance recognized three distinct categories of mobile applications. The first category consists of those mobile applications that do not meet the statutory definition of "device" in the Federal Food, Drug and Cosmetic Act (FD&C Act).[26] Because these mobile applications are not medical devices, the FDA does not regulate them. Mobile applications in this category include:

- Electronic copies of reference materials
- Educational tools, such as interactive anatomy diagrams
- Applications used for general patient education, such as information about gluten-free food products.[27]

The second category consists of those mobile applications that meet the statutory definition of "device," but are deemed to pose a low safety risk to the public. The intended use of a mobile application determines whether it meets the statutory definition of a "device." If the intended use of a mobile application is to diagnose a disease or other condition; to cure, mitigate, treat or prevent disease; or to affect the structure or any function of the body, then the mobile application falls within the definition of a device under the FD&C Act. For example, the FDA

---

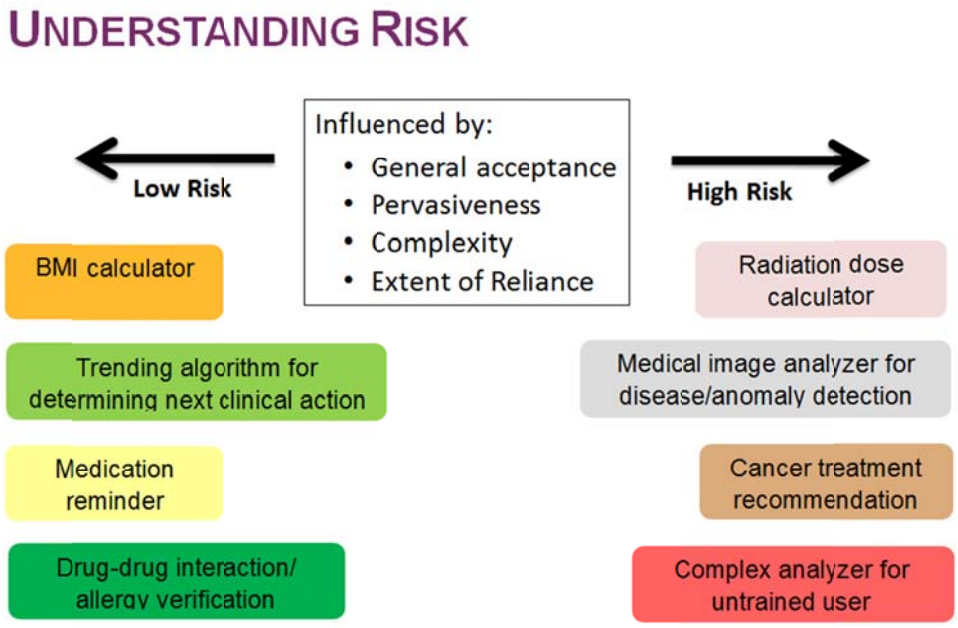
[25] FDA, "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" (Oct. 2, 2014), *available at* http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf [*hereinafter* FDA Cybersecurity Guidance].

[26] 21 U.S.C. § 301, et. seq.

[27] FDA Guidance, *supra* note 24, at 20.

explains that, if a mobile application makes a mobile device's light-emitting diode operate to illuminate objects generally, it is not a "device." However, if the intended use, which might be shown by labeling, advertising materials or oral or written statements of the manufacturer, is to provide a light source for doctors to examine patients, then the intended use of the mobile application would be similar to a conventional device, such as an ophthalmoscope, and the mobile application would, therefore, be defined as a "device" under the FD&C Act. [28]

The FDA has regulatory discretion over which devices it determines to enforce the FD&C Act requirements against. Because the second category of mobile applications does not present a significant risk to patient care if they do not function as intended, the FDA, at this time, is not enforcing FD&C Act requirements with regard to this category of mobile applications. Accordingly, the risk inherent in the use of the mobile application/device must be evaluated to determine whether a mobile application that qualifies as a device will fall into this second category. The risk involved with the use of each mobile application is influenced by a variety of factors, including the general acceptance, pervasiveness, complexity and extent of human reliance on the device.



Mobile applications in this lower risk second category include:

- Applications that provide periodic educational or other information to help individuals self-manage a specific condition *(e.g.,* smokers, recovering addicts, asthmatics, diabetics)

- Applications that track and store user-entered health data *(e.g.,* asthmatics, diabetics, medication information, fitness) and communicate with health care providers

[28] *Id.* at 8.

- Checklists of common signs and symptoms to provide advice on when to consult a physician

- Applications that automate basic tasks for health care providers.[29]

In recent years, interconnected mobile applications in this second category intended to log, record and track an individual's fitness, health and wellness, such as Fitbit and Apple's HealthKit, have helped to define an entirely new wearable market. Although not currently subject to FDA regulation as medical devices, these mobile applications collect personal health information that individuals can share with medical professionals to aid in treatment decisions. Collection of such personal information by the mobile applications is subject to FTC regulation, as described above, and, once incorporated into an electronic medical record, can become protected health information subject to regulation under HIPAA. Accordingly, manufacturers and users of mobile applications should be cognizant of other regulatory regimes that may apply to data collected by such mobile applications, even if such mobile applications are not subject to regulation by the FDA.

The third and final category of mobile applications consists of those mobile applications that meet the statutory definition of "device" and are intended (1) to be used as an accessory to a regulated medical device or (2) to transform a mobile platform into a regulated medical device. The FDA calls mobile apps in this category "mobile medical applications."[30]

The FDA confirmed in the FDA Guidance that it will regulate such mobile medical applications in the same way it would regulate traditional medical devices. Mobile applications in this category include:

- Applications that are intended to be used as an accessory to a medical device, connect to and control medical devices, or display, store, analyze or transmit patient-specific medical device data (*e.g.*, direct or remote control of insulin pumps or blood pressure cuffs or remote display of data from bedside monitors)

- Applications that transform the mobile platform into a medical device with attachments, sensors, etc. (*e.g.*, attachment of a blood glucose strip meter)

- Applications that perform patient-specific analysis, diagnosis, etc. (*e.g.*, to calculate dosage or create a dosage plan for radiation therapy).[31]

In summary, the FDA Guidance explains that the majority of mobile applications fit into the first two categories described above. As a practical matter, therefore, the FDA will not regulate most mobile applications. Rather, it will only regulate the third category (*i.e.*, "mobile medical applications.") However, mobile applications in any of the three categories may

[29] *Id.* at 23.

[30] *Id.* at 7.

[31] *Id.* at 27.

be used in a clinical environment. The question then becomes, how does one determine into which category their mobile application fits?

VII. Mobile Medical Applications Subject to FDA Regulation

As explained above, even if a mobile application meets the statutory definition of a "device," the FDA will not regulate it unless it is a "mobile medical application." Mobile medical applications are intended to be used as accessories to regulated medical devices or to transform a mobile platform into a regulated medical device, which poses a safety risk to the public if they do not function as intended. The FDA provides three broad examples of intended use that would make a mobile application a mobile medical application subject to FDA regulation.

The first are mobile applications that are used as extensions of one or more medical devices by connecting (physically or remotely) to such devices for purposes of controlling the devices or for use in active patient monitoring or analyzing medical device data. Examples of devices used in active patient monitoring or analyzing medical data include those displaying radiological images and remote displays of bedside monitors. Examples of mobile applications that control medical devices include mobile applications that provide the ability to control blood pressure cuffs or the delivery of insulin by an insulin pump. Mobile medical applications of this type are considered to be accessories to the connected devices and are required to comply with the regulatory controls applicable to those connected devices.[32]

The second type are mobile applications that transform the mobile platform itself (*e.g.*, an iPad or smartphone) into a regulated medical device by using attachments, display screens or sensors or by including functionality similar to that of currently regulated medical devices. Examples of such mobile applications include a mobile application that uses an iPad or a smartphone for medical device functions, such as by attaching a blood glucose strip reader so that the iPad or smartphone functions as a glucose reader and a mobile application that uses the built-in accelerometer to collect information to monitor a patient's sleep apnea. Mobile applications that use attachments, display screens, sensors or similar components are required to comply with the regulatory requirements applicable to the device classification associated with the type of device into which the mobile platform was transformed.[33]

The FDA had already begun to regulate this second category of mobile applications prior to the release of the FDA Guidance. For example, the FDA sent an "It has come to our attention" letter to mobile application manufacturer Biosense Technologies regarding its uChek Urine analyzer mobile application, citing its failure to obtain 510(k) clearance before marketing the mobile application.[34] The uChek Urine analyzer allowed a mobile phone to analyze certain FDA-cleared urine dipsticks. However, the dipsticks themselves were

---

[32] *Id.* at 28.

[33] *Id.* at 27.

[34] FDA, Letter to Biosense Technologies Private Limited concerning the uChek Urine Analyzer (May 24, 2013), *available at* http://www.fda.gov/MedicalDevices/ResourcesforYou/Industry/ucm353513.htm.

only cleared for direct visual analysis. Consequently, according to the FDA, because the mobile application provided automated reading, the mobile application and the dipsticks required new FDA clearance as a urinalysis test system. Therefore, even if a mobile application simply builds on existing devices to automate their operation, the mobile application will be subject to FDA regulation.

Finally, the third type is a mobile application that is a regulated medical device (software) in of itself because it performs patient-specific analysis and provides patient-specific diagnosis or treatment recommendations. Examples include mobile applications that perform sophisticated analysis or interpret data, whether collected electronically or manually, from another medical device, such as a mobile application that uses patient-specific information to calculate a dosage plan for radiation therapy and computer-aided detection software for medical-image processing.[35]

VIII. Consequences of FDA Regulation

Mobile medical applications are subject to the same regulatory requirements as traditional medical devices. Accordingly, for mobile medical applications, manufacturers must meet the requirements associated with the device classification applicable to the mobile medical application. Mobile medical application manufacturers may include anyone who initiates specifications, designs, labels or creates a mobile medical application, thereby potentially subjecting health care organizations, facilities and practitioners that procure or develop mobile applications from third-party providers of software development services to FDA regulatory requirements. In addition, mobile medical application manufacturers should adhere to the FDA Cybersecurity Guidance related to software such as mobile medical applications, as described below.

A mobile medical application, like other devices, may be classified as class I (subject to general controls), class II (subject to special controls in addition to general controls), or class III (subject to premarket approval requirements).[36] In general, mobile medical application manufacturers are subject to the following regulatory requirements, depending on the classification of the mobile medical application:

- Establishment Registration and Medical Device Listing: Manufacturers of mobile medical applications must register their establishments with the FDA. In addition, manufacturers must list their mobile medical applications and other devices with the FDA.

- Investigational Device Exemption (IDE) Requirements for Clinical Studies: A manufacturer may wish to use a mobile medical application or other device in a clinical study to collect data regarding the safety and effectiveness of the mobile medical application or device prior to submission of a premarket notification or

[35] FDA Guidance, *supra* note 24, at 29.

[36] *See id.* at 19 (providing an overview of regulatory requirements for each class and a link to helpful classification guidance).

premarket approval application. In order to do so, a manufacturer must obtain an IDE. Clinical studies with devices of significant risk must be preapproved by the FDA and an institutional review board; while studies with devices of nonsignificant risk must be approved only by an institutional review board prior to performing the study.

- Labeling Requirements: Mobile medical applications must comply with FDA labeling requirements for device labels and all descriptive and informational literature that accompanies the mobile medical application.

- Premarket Submission for Approval or Clearance: If the device classification applicable to the mobile medical application requires the submission of a premarket notification, a manufacturer cannot commercially distribute the mobile medical application until the FDA provides a letter of substantial equivalence authorizing the manufacturer to do so. Most class I and class II devices are exempt from the premarket notification requirements. Mobile medical applications that are high-risk devices that pose a significant risk of illness or injury or those found not to be substantially equivalent to class I and class II devices must go through the premarket approval process. The premarket approval process is more involved than the notification process and includes submission of clinical data to support claims made for the device.

- Quality System Regulation: Mobile medical applications must comply with the Quality System regulation, which includes requirements related to the controls used for designing and manufacturing devices. The FDA strongly recommends that manufacturers of all mobile health care applications, not just mobile medical applications subject to FDA regulation, follow the Quality System regulation in the design and development of their mobile applications and initiate prompt corrections to their mobile applications, when appropriate, to prevent patient and user harm.[37]

- Medical Device Reporting: Manufacturers are required to report adverse events that may have caused or contributed to death or serious injury as well as certain malfunctions.

IX. FDA Cybersecurity Guidance for Manufacturers

Internet- and network-connected life-saving and life-enhancing medical devices, such as pacemakers and patient monitors, are vulnerable to hackers and other cybersecurity threats. Exploitation of these vulnerabilities could have potentially catastrophic impacts on the safety of the patients who rely on those devices.[38] To address these concerns, the FDA issued its

[37] *Id.* at 13.

[38] Out of a concern over the potential for assassination attempts via hacking, Dick Cheney's doctor had ordered the former vice president's heart implant's wireless capability disabled while he was in office. *See* Andrea Peterson, "Yes, Terrorists Could Have Hacked Dick Cheney's Heart," *The Washington Post* (Oct. 21, 2013),

FDA Cybersecurity Guidance, which provides cybersecurity recommendations that medical device manufacturers should consider in the design and development of interconnected medical devices and in preparing premarket submissions for such medical devices. On January 15, 2016, the FDA expanded its cybersecurity efforts to approved medical devices by issuing draft guidance on the Postmarket Management of Cybersecurity in Medical Devices (Postmarket Guidance).[39]

A. General Cybersecurity Principles

The FDA Cybersecurity Guidance recommends that manufacturers develop a set of cybersecurity controls to assure medical device cybersecurity and maintain medical device functionality and safety.[40] Consistent with the "privacy by design" approach and the application of sound security principles in new product design recommended by the FTC, the FDA urges manufacturers to address cybersecurity during the design and development of a medical device to achieve more robust and efficient mitigation of risks to patients. The FDA lays out a recommended approach that includes a thorough risk analysis. As part of that recommended approach to cybersecurity, a manufacturer should address the following: (1) the identification of assets, threats and vulnerabilities; (2) an assessment of the impact of threats and vulnerabilities on device functionality and patients; (3) an assessment of the likelihood of a threat and of a vulnerability being exploited; (4) a determination of risk levels and suitable mitigation strategies; and (5) an assessment of residual risk.[41]

In a draft version of the FDA Cybersecurity Guidance from 2013, the FDA stated that manufacturers should implement measures to ensure the confidentiality, integrity and availability of information stored on medical devices. Although reference to these well-known "CIA of information" principles did not make it into the final guidance, these principles permeate and underlie many of the standards recommended in the FDA Cybersecurity Guidance. Accordingly, manufacturers should continue to address these principles in their approach to cybersecurity.

B. Cybersecurity Functions

To guide cybersecurity activities, the FTC recommends that medical device manufacturers consider the cybersecurity framework core functions recommended by the National Institute of Standards and Technology in its Cybersecurity Framework for Critical

---

available at https://www.washingtonpost.com/news/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/.

[39] FDA, "Postmarket Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff" (Jan. 2016), *available at* http://assets.law360news.com/0747000/747440/post_market_cybersecurity_draft_guidance.pdf.

[40] FDA Cybersecurity Guidance, *supra* note 25, at 3.

[41] *Id.* at 4.

Infrastructure. Generally, these include identify, protect, detect, respond and recover.[42] Many concepts in this framework overlap with the data security concepts recommended by the FTC in its IoT Report, such as "security by design" and monitoring threats and vulnerabilities throughout a product's life cycle.[43]

To "identify" and "protect," manufacturers should assess a device's vulnerability to cybersecurity threats. The extent to which security controls are needed depends on the intended use of the device; whether it is capable of connecting to the Internet, a network or another device; and the likelihood of patient harm that would result from a cybersecurity breach. Manufacturers should provide justifications in their premarket submissions for the security functions chosen for their medical devices. The FDA recommends that all manufacturers fulfill the "identify" and "protect" core functions.[44] Security controls recommended by the FDA to fulfill these functions include:

- Limit Access to Trusted Users
    - Limit access to devices through the authentication of users (*e.g.*, user ID and password, smartcard, biometric).
    - Use automatic timed methods to terminate sessions within the system where appropriate for the use environment.
    - Where appropriate, employ a layered authorization model by differentiating privileges based on the user role (*e.g.*, caregiver, system administrator) or device role.
    - Use appropriate authentication (*e.g.*, multifactor authentication to permit privileged device access to system administrators, service technicians and maintenance personnel).
    - Strengthen password protection by avoiding "hardcoded" passwords or common words (*i.e.*, passwords that are the same for each device, difficult to change, and vulnerable to public disclosure), and limit public access to passwords used for privileged device access.
    - Where appropriate, provide physical locks on devices and on their communication ports to minimize tampering.

[42] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity" (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

[43] IoT Report, *supra* note 16.

[44] FDA Cybersecurity Guidance, *supra* note 25, at 4.

- Require user authentication or other appropriate controls before permitting software or firmware updates, including those affecting the operating system, applications and anti-malware.

- Ensure Trusted Content

  - Restrict software or firmware updates to authenticated code. One authentication method manufacturers may consider is code signature verification.

  - Use systematic procedures for authorized users to download version-identifiable software and firmware from the manufacturer.

  - Ensure the capability of secure data transfer to and from the device, and, when appropriate, use methods for encryption.

To "detect, respond and recover," the FDA recommends that manufacturers consider the following security controls:

- Implement features that allow for security compromises to be detected, recognized, logged, timed and acted on during normal use.

- Develop and provide information to the end user concerning appropriate actions to take upon detection of a cybersecurity event.

- Implement device features that protect critical functionality, even when the device's cybersecurity has been compromised.

- Provide methods for retention and recovery of device configuration by an authenticated privileged user.[45]

C. Cybersecurity Documentation

The FDA Cybersecurity Guidance recommends that manufacturers submit certain information related to the device's cybersecurity controls in premarket submissions. This information includes the following: (1) the manufacturer's hazard analysis, mitigations and design considerations pertaining to intentional and unintentional cybersecurity risks; (2) a traceability matrix that links cybersecurity controls to the risks considered; and (3) a plan for providing validated software updates and patches and instructions for use and product specifications for the device related to recommended cybersecurity controls for the intended use environment, such as anti-virus software and firewalls.[46]

[45] *Id.* at 5.

[46] *Id.* at 6.

D. Postmarket Management of Cybersecurity

The Postmarket Guidance, which is subject to a 90-day comment period, identifies the steps that manufacturers of networked medical devices should take to identify and address postmarket cybersecurity vulnerabilities that pose a risk to patient safety and public health. In addition, this guidance identifies which cybersecurity-related vulnerabilities and changes manufacturers must report to the FDA and encourages the sharing of cybersecurity threat information as part of the postmarket surveillance process. Recognizing that it is not possible to completely mitigate risks through premarket controls alone, the FDA recommends that manufacturers promptly implement a cybersecurity risk management program to:

- Monitor cybersecurity information sources to identify and detect vulnerabilities and risks
- Detect, assess and understand the presence and impact of a vulnerability
- Establish and communicate processes for handling vulnerabilities
- Develop mitigations to protect, respond and recover from risks
- Adopt a vulnerability disclosure policy and practice
- Develop preventive measures to mitigate and address risks early and prior to exploitation.

According to the FDA, a key purpose of conducting the risk management assessment portion of this program is to determine whether cybersecurity vulnerabilities pose a risk to clinical performance that is "controlled" or "uncontrolled." A controlled risk is defined as one where there is a sufficiently low residual risk that cybersecurity vulnerabilities could compromise the device's clinical performance; whereas, an uncontrolled risk poses an unacceptable risk that performance could be compromised. The extent of a manufacturer's reporting obligations depends on whether a risk is classified as "controlled" or "uncontrolled." The FDA requires heightened reporting for uncontrolled risks. Specifically, the FDA indicated that manufacturers would not generally need to report efforts taken "solely to strengthen cybersecurity" related to a controlled risk, but would be required to report actions taken in connection with an uncontrolled risk. The FDA noted, however, that it does not intend to enforce the 21 C.F.R. part 806 reporting requirements for uncontrolled risk where the following conditions are met:

- The vulnerability does not result in serious adverse events or deaths.
- The manufacturer notifies users of the risk and takes steps to bring it to an acceptable level within 30 days of learning of the vulnerability.
- The manufacturer currently participates in an Information Sharing Analysis Organization.

The Postmarket Guidance also provides recommendations on how manufacturers of mobile medical applications and other medical devices should report cybersecurity risks, whether controlled or uncontrolled, as part of their annual reporting requirements.

E. Cybersecurity and the Medical Device Consumer

Recent actions by the FDA also show its growing concern about, and attention to, cybersecurity issues. On July 31, 2015, the FDA issued a safety communication to health care facilities to alert users of the Hospira Symbiq System to cybersecurity vulnerabilities with one of Hospira's infusion pumps.[47] According to the alert, an unauthorized user could potentially access the pump remotely to alter the dosage it delivers, which could lead to over-infusion or under-infusion of critical patient therapies. The FDA strongly encouraged health care facilities to discontinue the use of the vulnerable pumps and transition to alternate pumps as soon as possible. This is the first time that the FDA has recommended discontinuing the use of a specific medical device based on cybersecurity concerns, which indicates the importance that the FDA will be placing on cybersecurity issues going forward.

Consequently, the current FDA regulatory environment related to cybersecurity is one that affects both manufacturers and consumers of mobile medical applications and other medical devices. Manufacturers of mobile medical applications and other medical devices should adhere to the detailed programmatic recommendations related to cybersecurity when bringing a mobile medical application to market. On the other hand, consumers of mobile medical applications and other medical devices, such as health care facilities, need to ensure that their information security programs include mechanisms to stay up to date on FDA cybersecurity alerts and that they are taking appropriate measures to address the vulnerabilities identified by the FDA. Health care facilities that do not respond appropriately to such warnings could find themselves suffering reputational harm and incurring significant legal and financial consequences in the event of a cyberattack that exploited such vulnerabilities.

X. Practical Takeaways

The regulatory landscape surrounding mobile medical applications is complex and likely to change as guidance from federal agencies continues to evolve and overlap. Even if a mobile application is not currently subject to FTC or FDA regulation, the mobile application may be subject to other federal and state agency regulations. Consequently, organizations should implement appropriate policies and procedures aimed at addressing and documenting their compliance with current and evolving regulatory standards. As part of such policies and procedures, organizations should consider the following:

- Appointment of a Committee to Monitor Relevant Regulatory Guidance: Federal and state regulatory agencies are extremely active in the privacy and data security space, and the FTC's successful action against Wyndham confirmed that regulatory enforcement can occur in the absence of an agency's publication of a comprehensive set of step-by-step privacy and cybersecurity rules. Accordingly, it

[47] FDA, "Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication" (July 31, 2015), available at http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm456815.htm.

is the responsibility of the health care organization to keep up with each agency's requirements. To maintain an adequate understanding of evolving regulatory standards, organizations should appoint a committee (or individual) tasked with the responsibility of keeping the organization up to date. New guidance or alerts may mean an organization should reevaluate its response plans and procedures or transition away from the use of a device with known vulnerabilities.

- Look for Common Compliance Principles Across Regulatory Agencies: Keeping track of regulatory requirements across multiple agencies and having to check the box for each of those agencies' various requirements can be daunting. However, much of the regulation from each of the disparate agencies is rooted in similar compliance principles. For example, the FTC has stated that products should be developed with privacy by design and sound security principles. Similarly, the FDA recommends addressing security in the design and development phase. Both agencies recommend that secure passwords and appropriate authentication mechanisms be used. By determining where the regulatory requirements of different agencies are effectively the same, your organization can more easily determine which exceptions deserve focus based on the compliance regime(s) the organization expects to apply to the mobile application.

- Follow and Document Privacy, Security and Quality Principles: In addition to assisting with overall compliance, documentation may help an organization demonstrate to a regulatory agency that it has engaged in privacy and security practices that were reasonable and in conformance with the organization's regulatory obligations.

- Perform and Update Risk Analyses for Privacy and Security: Assessing threats and vulnerabilities is a necessary step to remediating identified risks.

- Obtain Consent for the Collection of Personally Identifiable Information: Development of the consent disclosures required to obtain the informed consent to collect and use an individual's personally identifiable information can, in addition to assisting an organization in meeting its privacy obligations, present an excellent opportunity to assess what information is being collected and for what purpose it is being used. This can allow an organization to ensure it is collecting only personally identifiable information that it needs and is using it only for legitimate business purposes within the contemplation of the individual providing the information.

- Take Precautions to Prevent and Eliminate Malware Contamination: Organizations should use industry-accepted anti-virus tools and install security updates supplied by software manufacturers. Many high-profile breaches have been caused by a failure to keep software security up to date.

- Monitor Network Connectivity for Misuse: Utilize an intrusion detection system and monitor system logs for suspicious activity.

- Analyze New Products for Regulatory Compliance: Both the FTC and the FDA recommend that privacy and security be addressed in the design and development phase when creating new products, such as mobile applications. Organizations should conduct a privacy and security impact assessment for each new mobile application to assess personal data collection, use, sharing, storage and disposal and assess threats and vulnerabilities so that the organization can select security controls that are appropriate for the new mobile application.

- Educate Mobile Application Developers on Regulatory Lines: It is most efficient (and consistent with regulatory guidance) to address privacy and security issues up front in the design and development phase. Education of developers regarding the triggers for regulatory compliance can help the organization to identify issues and solutions earlier.