Houston Journal of Health Law & Policy

MOBILE MEDICAL APPS: WHERE HEALTH AND INTERNET PRIVACY LAW MEET

Barbara Fox

TABLE OF CONTENTS

I. INTRODUCTION 193
II. LAW AND TECHNOLOGY 195
A. Changing Face of Healthcare 195
B. The Medical Industry Takes Interest 197
C. Health and Safety: What is the FDA Doing? 197
D. Current FDA Regulations 199
E. Guidance for Mobile Medical Applications 202
F. FDA Regulations – Conclusion 205
III. PRIVACY CONCERNS 205
A. Mobile Medicine and Privacy 206
B. Electronic Health Records and Personal Health Records 208
C. Psychological and Progressive Conditions 210
IV. INTERNET, PRIVACY, AND MOBILE MEDICINE 211
A. HIPAA and Mobile Medical Technology 213
B. HITECH and Beyond: What Remedies Other Areas of Law Offer 215
V. CONCLUSION 220

I. INTRODUCTION

The introduction of Apple's iPhone in 2007 revolutionized the mobile industry. In less than a decade, smartphones, such as the iPhone and the Android, changed life as we know it. No longer

isolated individuals, smartphone users now have entertainment, information, and everything in between at their fingertips. Recently, doctors, pharmacists, and companies have banded together to develop applications ("apps") that promise to redefine the way medicine is practiced. It is hoped that apps will help users manage their health on a day-to-day basis.

However, there are a number of concerns surrounding the use of apps in the medical field. First, the FDA has not yet passed guidance specifically aimed at mobile medical apps. In 2011 guidelines were introduced for comment.[1] Under the guidelines, apps are treated as accessories rather than independent entities. Before mobile medical apps can be released safely into the market, more concrete standards specifically tailored to mobile apps must be in place.

Mobile medical apps often contain the equivalent of electronic medical records; therefore questions arise regarding what should be done to protect user information stored by the app. Mobile medical apps exceed the scope of the Health Insurance Portability and Accountability Act (HIPAA), so users will have to look to other areas of the law for protection. One potential avenue for protection lies within the realm of Internet Privacy law.[2]

With this problem in mind, Part I will provide a general introduction to the relationship between healthcare and mobile technology, specifically the first wave of medical mobile apps. Part II will focus on the current regulatory structure for medical technology, including the FDA's guidelines regarding mobile medical apps. Part III will address the privacy protections currently in place, and the limitations on HIPAA. Part IV will recommend a cross-discipline approach, fusing Internet privacy law and health law, for further regulation.

---

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

[2] Kathryn McEnery, *The Usefulness of Non-linear Thinking: Conceptual Analysis Tools and an Opportunity to Develop Electronic Health Information Privacy Law,* 23 HEALTH LAW 18, 18 (2010).

II. LAW AND TECHNOLOGY

Over the past 30 years technology has developed at an astonishing rate. In many ways the technology "boom" has outpaced the law.[3] This is particularly true concerning the Internet and personal mobile technology.[4] As these areas continue to develop, legal implications surrounding them become increasingly complex.[5] One central concern is the development of a comprehensive and cohesive regulatory scheme that will appropriately address this type of technology now and as it evolves.

A. Changing Face of Healthcare

The past few decades have seen an increased awareness of the number of Americans living with chronic health conditions such as obesity,[6] diabetes,[7] bipolar disorder,[8] obsessive-compulsive disorder (OCD),[9] and post-traumatic stress disorder (PTSD).[10] One common

---

[3] Lyria Bennett Moses, *Recurring Dilemmas: The Law's Race to Keep Up with Technological Change*; 2007 U. Ill. J.L. TECH. & POL'Y 239, 243 (2007). Moses identifies four types of legal problems that arise from new technology:

> "(1) the potential need for laws to ban, restrict, or, alternatively, encourage a new technology; (2) uncertainty in the application of existing legal rules to new practices; (3) the possible over-inclusiveness or under-inclusiveness of existing legal rules as applied to new practices; and (4) alleged obsolescence of existing legal rules."

[4] *Id.*

[5] *Id.* Complexity in this area increases as the areas of health, internet, and privacy law continue to fuse as technology continues to develop and outpace the law. *Id.*at 256–56.

[6] CYNTHIA L. OGDEN et al., CTR. FOR DISEASE CONTROL AND PREVENTION, PREVALENCE OF OBESITY IN THE UNITED STATES, 2009 – 2010 (2012), *available at* http://www.cdc.gov/nchs/data/databriefs/db82.pdf. An estimated 1/3 of adult Americans are obese.

[7] *National Diabetes Fact Sheet*, CTR. FOR DISEASE CONTROL AND PREVENTION (2011)*available at*http://www.cdc.gov/diabetes/pubs/pdf/ndfs_2011.pdf. In 2010 approximately 1.9 million people 20 years or older were diagnosed with diabetes. *Id.*

[8] *The Numbers Count: Mental Disorders in America*, NATIONAL INSTITUTE OF MENTAL HEALTH, *available at* http://www.nimh.nih.gov/health/publications/the-numbers-count-mental-disorders-in-america/index.shtml#OCD. Bipolar disorder affects approximately 2.6 percent of the U.S. population in any given year. *Id.*

[9] *Id.* This includes approximately 2.2 million American adults aged 18 and older. *Id.*

[10] *Id.* "Approximately 7.7 million American adults age 18 and older, or about 3.5 percent of

element between these conditions is the need for long-term monitoring and treatment.[11] For conditions such as obesity, there has been a movement towards preventative care in hopes of reducing the number of patients developing greater complications.[12] That has generated programs such as the "Let's Move!" campaign and other initiatives to help Americans on their way to a healthier lifestyle.[13] As these programs evolved, developers turned to the mobile technology that has become commonplace in American society.

What researchers created was not new to the market. Previously there were a handful of apps in iTunes and Android markets, but their functions were limited.[14] However, numbers quickly soared as developers released fitness and diet related apps.[15] The market was quickly flooded with a mix of beneficial and ineffective apps promising to do the same thing: improve the user's health and quality of life.[16] These apps were developed and sold in a more or less unregulated market,[17] and they were followed by allegations of misrepresentation—most recently against a company claiming their app could "treat" acne by causing the cellphone to emit a special

---

people in this age group in a given year, have PTSD." *Id.*

[11] *See Chronic Diseases: The Power to Prevent, the Call to Control: At a Glance 2009*, CTRS. FOR DISEASE CONTROL AND PREVENTION, *available at* http://www.cdc.gov/chronicdisease/resources/publications/aag/chronic.htm. The CDC estimates that "75% of health care costs are due to chronic illness." *Id.*

[12] *See The Power of Prevention*, CTR. FOR DISEASE CONTROL AND PREVENTION, *available at* http://www.cdc.gov/chronicdisease/pdf/2009-power-of-prevention.pdf.

[13] *About Let's Move*, LET'S MOVE, http://www.letsmove.gov/about (last visited Mar. 13, 2013).

[14] *See* ERIC TOPOL, THE CREATIVE DESTRUCTION OF MEDICINE: HOW THE DIGITAL REVOLUTION WILL CREATE BETTER HEALTH CARE, 62 (Basic Books 2012). *See also* AlexKrouse, *IPads, IPhones, Androids, and Smartphones: FDA Regulation of Mobile Phone Applications as Medical Devices*, 9 Ind. Health L. Rev. 731, 745 (2012).

[15] Some estimates reach as high as 40,000 available health related apps. *See* Mohana Ravindranath, *Happtique Helps Doctors Prescribe Apps to Patients*, WASH. POST, Aug. 28, 2012, http://articles.washingtonpost.com/2012-08-28/news/35492027_1_smartphone-apps-welldoc-mhealth.

[16] *Id.* ("There are thousands of health-related apps available for download today on smartphones and tablets (by some estimates there could be as many as 40,000, though no formal count as been done.)").

[17] *Id.* ("There is little regulation of the industry. The Food and Drug Administration only Regulates medical mobile applications that accompany medical devices.").

light.[18]

B. The Medical Industry Takes Interest

With this in mind, physicians and pharmaceutical companies joined forces to do in a regulated way what had been attempted many times before: develop mobile technology that could help the individual user monitor and maintain their health. What they developed goes beyond one-sided monitoring, researching, and prevention of illness.[19]They created a platform that has the potential to redefine the doctor-patient relationship.[20]

The newly-developed, independent medical app market is still in the testing (or "beta") stages.[21] Before purchasing a medical app, patients are required to have a valid prescription from their doctor, just like any other prescribed medication or regimen.[22] Apps currently on the market are designed to treat chronic conditions, such as rheumatoid arthritis, obesity, diabetes, manic-depressive bipolar disorder, and PTSD.[23]

C. Health and Safety: What is the FDA Doing?

As part of the digital revolution, use of digitized medical records and diagnostic tools over the Internet has dramatically increased.[24]

---

[18] *"Acne Cure" Mobile APP Marketers Will Drop Baseless Claims Under FTC Settlements*, 13 No. 10 E-COMMERCE L. REP. 20 (Oct. 2011) (involving a settlement for two companies that misrepresented scientific data supporting the effectiveness of their acne treating apps).

[19] *See, e.g.*, Greg Reger, *Smart Phones, Service Members &PTSD Treatments*, NAT'L CENTER FOR TELEHEALTH & TECH., http://www.t2health.org/news/smart-phones-service-members-ptsd-treatments (last visited Mar. 13, 2013) (describing PE Coach, a mobile app designed to help veterans suffering from PTSD through basic assignments and at home therapy exercises accompanying therapy).

[20] *See, e.g., id.*

[21] Ravindranath, *supra* note 15, at 2 (describing a program that would allow doctors to locate a specific app on his smartphone/device, and "prescribe" an app to a specific patient via email).

[22] *Id.*

[23] *Id.; see also* Joshua Brustein, *Coming Next: Using an App as Prescribed*, N.Y. TIMES, Aug. 19, 2012, http://www.nytimes.com/2012/08/20/technology/coming-next-doctors-prescribing-apps-to-patients.html?smid=pl-share.

[24] Elana Rivkin-Haas, *Electronic Medical Records and the Challenge to Privacy: How the United*

Concerns quickly arose over the quality and reliability of services, and the ability to restrict access to those services to specified users.[25] For example, if a medical diagnosis is to be made beyond arm's length, then extra precautions are needed to ensure that the "cyber-doctor" is actually board certified and qualified in the area of practice.[26] Additional measures were implemented to ensure the use of reliable diagnostic methods.[27] With the dawn of online pharmacies, safeguards were implemented to ensure that the pharmacy was complying with federal and state law, that prescriptions were valid, and that the drugs being marketed were not counterfeit.[28] The risk was high that such a tool could be used to circumvent the usual prescription and quality regulation process and create an illegal drug market or grave risk of injury to the patient.

As with any new technology, there are concerns surrounding the risks of mobile medical apps.[29] The principal focus is on the quality

States and Canada are Responding, 34 HASTINGS INT'L& COMP. L. REV. 177, 178 (2011).

[25] 21 C.F.R. § 860.3 (2008); 21 C.F.R. § 860.7 (2008); Brustein, *supra* note 23.

[26] Parallels can be drawn to the practice of tele-medicine, or cyber-medicine, at the start of the new millennium. One key problem in this area is that states have inconsistent licensure requirements before a doctor can practice cyber-medicine. According to Lisa Rannefeld:

> "For the interstate practice of medicine, physicians are unclear whether they must obtain licenses to practice in the state where patients are located or in the state in which they are practicing. States generally adopt one of four approaches: (1) out-of-state practitioners cannot provide care if they do not have a full license to practice within the state; (2) "limited" licenses for telemedicine; (3) statutes that promote telemedicine for specific types of care; and (4) out-of-state providers can render care, provided it is rendered through in-state providers and provided the in-state providers control patient care."

Lisa Rannefeld, The Doctor will E-Mail you Now: Physicians' Use of Telemedicine to Treat Patients Over the Internet, 19 J.L. & HEALTH 75, 92 (2005).

[27] *See id.*

[28] *See id.* at 89. ("According to the AMA, prescriptions issued over the Internet often fail to meet appropriate standards of care. The AMA states that quality is sacrificed because:

> [1] there are no examinations of the patient to determine if there is a medical problem and to determine a specific diagnosis; [2] there is no dialogue with the patient to discuss treatment alternatives and to determine the best course of treatment; [3] there is no attempt to establish a reliable medical history; [4] there is no provision of information about the benefits and risk of the prescribed medication; and [5] there is no follow-up to assess the therapeutic outcome.").

[29] Vernessa T. Pollard, *FDA Medical Device Requirements: A Legal Framework for Regulating Health Information Technology, Software, and Mobile Apps*, 2011 WL 5833341 (Nov. 2011).

and safety of each product that enters the market, and the measures that can be taken to ensure user safety.[30] When dealing with digital technology, the investigation takes on a whole new approach. Compared to surgical instruments, the harms of mobile medical devices are not obvious, but that does not mean they are not present.[31] What distinguishes apps from traditional medical equipment is that apps are placed in the hands of patients, not surgeons. When the instrument is in the patient's control, there is less opportunity to correct operating errors before they cause injuries.

D. Current FDA Regulations

Guidance specifically aimed at controlling the safety and quality of mobile medical apps was approved in September 2013, and has not been extensively applied.[32]Until recently, the only guidance available to app developers was found in 21 C.F.R. § 860, which delineates the procedures by which the FDA will classify medical devices for approval. However, before a device can be categorized, the evaluating committee must consider a number of soft factors including the intended use and the user, the risks and benefits of the device, and the reliability of the device.[33] Once those elements have

"There is a significant concern and a lack of definition around what constitutes an adverse event for health IT products. If these systems do not function as intended and the patient has an adverse health outcome, there is some lack of clarity in deciding what would be considered an adverse health outcome associated with a mobile app or software, and/or how to determine whether health-related IT, software, or a mobile app was a factor in that injury. Further, the FDA has suggested that medical device reports for health IT should include information concerning malfunctions or injuries that are attributable to malware or viruses or associated with the device."*Id.*

[30] 21 C.F.R. § 860.3 (2008); 21 C.F.R. § 860.7 (2008); *see also* Brustein, *supra* note 23, at 1 ("[U]nlike a 99-cent game, apps dealing directly with medical care cannot be introduced to the public with bugs that will be fixed later. The industry is still grappling with how to ensure quality and safety.").

[31] *See* Pollard, *supra* note 29.

[32] Guidance for Industry and Food and Drug Administration Staff, *supra* note 1.

[33] 21 C.F.R. § 860.7(b) (2008) states:

> (b) In determining the safety and effectiveness of a device for purposes of classification, establishment of performance standards for class II devices, and premarket approval of class III devices, the Commissioner and the classification panels will consider the following, among other relevant factors:
>
> (1) The persons for whose use the device is represented or intended;

been ascertained, the device can be more readily analyzed and appropriately classified as Class I, II, or III, discussed below.[34]

Class I medical devices meet the minimal level of safety standards in order to be released to the public.[35,36]So long as the device does not pose a threat to life or limb, it is required only to meet minimal standards prohibiting adulteration, misbranding and other general regulations.[37]The benefit of this low threshold is that pre-market approval is not required.[38]

Class II medical devices are minimally dangerous, but are usually more invasive than Class I devices.[39] This category is subject to the same general standards as Class I, but must additionally

---

> (2) The conditions of use for the device, including conditions of use prescribed, recommended, or suggested in the labeling or advertising of the device, and other intended conditions of use;
>
> (3) The probable benefit to health from the use of the device weighed against any probable injury or illness from such use; and
>
> (4) The reliability of the device.

[34] 21 C.F.R. § 860.3 (2008).

[35] 21 C.F.R. § 860.3(c)(1) (2008) states:

> A device is in class I if (i) general controls are sufficient to provide reasonable assurance of the safety and effectiveness of the device, or (ii) there is insufficient information from which to determine that general controls are sufficient to provide reasonable assurance of the safety and effectiveness of the device or to establish special controls to provide such assurance, but the device is not life-supporting or life-sustaining or for a use which is of substantial importance in preventing impairment of human health, and which does not present a potential unreasonable risk of illness of injury.

[36] Classic examples of Class I devices include bandages, examination gloves, and hand-held surgical instruments. *See Regulatory Controls*, U.S. FOOD AND DRUG ADMINISTRATION, *available at* http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/GeneralandSpecialControls/default.htm (last updated Apr. 11, 2013).

[37] 21 C.F.R. § 860.3(c)(1) (2008).

[38] *Overview of Device Regulation*, U.S. FOOD AND DRUG ADMIN., http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/default.htm (last updated Apr. 11, 2013). *See also Class I Medical Devices and Class II Medical Devices*, COUGHLIN COMPANIES, INC., http://www.coghlincompanies.com/Cogmedix/cogmedix_class_I_class_II.php (last visited Mar. 13, 2013).

[39] Examples include x-ray machines, powered wheel chairs, infusion pumps, surgical needles, and suture materials. *Class I Medical Devices and Class II Medical Devices*, *supra,* note 38.

comply with "performance standards, post market surveillance, patient registries, development and dissemination of guidance documents, . . . recommendations, and other appropriate actions as the Commissioner deems necessary."[40] These additional standards vary from device to device and give the approval committee leeway in determining whether an individual piece of equipment is suitable for use.[41] That leeway is especially clear when the committee engages inpost market surveillance. When utilizing post market surveillance, the committee continues to monitor data collected over time from use of the device in the open market.[42] If, after a period of time, the committee finds that the device has hidden risks that were not evident at the time of initial approval, the device can be re-categorized and thereby subject to more stringent regulations.[43]

Class III medical devices pose the greatest risk to human life and must, therefore, surpass the most rigorous standards before they can be introduced into the market.[44] In addition to all of the hurdles Class I and Class II devices must satisfy, Class III devices are subjected to pre-market approval.[45] The broadest range of devices falls within this

[40] 21 C.F.R. § 860.3(c)(2)(2012)(defines Class II medical devices as "Class II means the class of devices that is or eventually will be subject to special controls. A device is in class II if general controls alone are insufficient to provide reasonable assurance of its safety and effectiveness and there is sufficient information to establish special controls, including the promulgation of performance standards, post-market surveillance, patient registries, development and dissemination of guidance documents (including guidance on the submission of clinical data in premarket notification submissions in accordance with section 510(k) of the act), recommendations, and other appropriate actions as the Commissioner deems necessary to provide such assurance").

[41] *See* 21 C.F.R. § 860.3(g)(2012).

[42] *Id.*

[43] 21 C.F.R. § 860.123 (2012).

[44] Examples of Class III medical devices include pacemakers, defibrillators, surgical reconstruction components, and artificial joint implants. *Class III Medical Devices*, FMI, http://www.fmimed.com/class-3-medical-devices.html (last visited Mar. 13, 2013).

[45] 21 C.F.R. § 860.3(c)(3) (2012) (defining Class III medical devices as "Class III means the class of devices for which premarket approval is or will be required in accordance with section 515 of the act. A device is in class III if insufficient information exists to determine that general controls are sufficient to provide reasonable assurance of its safety and effectiveness or that application of special controls described in paragraph (c)(2) of this section would provide such assurance and if, in addition, the device is life-supporting or life-sustaining, or for a use which is of substantial importance in preventing impairment of human health, or if the device presents a potential unreasonable risk of illness or injury").

third category, including devices without sufficient data to place them in a lesser category as well as those that truly threaten injury. While some truly dangerous equipment is classified as Class III, by and large it is a cautionary category where devices are essentially held for observation before being reclassified as a lower division.[46]

E. Guidance for Mobile Medical Applications

The FDA has approved a rigid classification system based on the risk of physical harm from a medical device parallel to what exists for medical equipment.[47]For the most part, that classification is precisely what the medical field requires. However, when the potential harm is not just physical, what should be done? Mobile medical apps occupy a grey area because they do not necessarily pose an imminent physical danger, but have the potential to cause great physical and psychological harm.

In the fall of 2013, the FDA approved guidelines for mobile medical technology.[48] The guidelines are designed to address the question of how mobile medical apps are to be regulated.[49] The guidelines took a number of novel approaches to the concept of mobile medical apps, including the requirement that each appmeet the definition of "device" in section 201(h) of the Federal Food, Drug, and Cosmetic Act (hereinafter FDCA)[50, 51]Additionally, the guidelines introduced the requirement that the mobile medical apps must be "used [either] as an accessory to a regulated medical device, or transform[] a mobile platform into a regulated medical device."[52] In a latter section of the guidance, the drafters provide a third option for mobile medical apps, in which the app functions independently of

[46] 21 C.F.R. § 860.136 (2012); 21 C.F.R.860.3(c) (2008)

[47] Guidance for Industry and Food and Drug Administration Staff, *supra* note 1.The guidance specifically provides for a three class division, similar to the way other medical devices are categorized. *Id.* at 19.

[48] *Id.*

[49] *Id.* at 19.

[50] *Id.* at 7.

[51] 21 U.S.C. § 321(h) (2009) (defining "device").

[52] Guidance for Industry and Food and Drug Administration Staff, *supra* note 1., at 7.

another medical device.[53] Each will be addressed in turn.[54]

Under the first approach, a mobile medical app would be considered an accessory, or an "extension," of whatever medical device it is associated with.[55]Under 21 C.F.R. § 860.7, the individual device would have its own standard for quality and safety, and any associated app would have to satisfy the same standard.[56]However, the drafters recognized the limitations of such a rigid classification system.[57] By categorizing an app through the device it enhances, there is a risk of restricting an app that does no more than transmit or store information. The drafters attempted to ameliorate the problem by allowing apps that merely aid in the use of a device, rather than enhance its functionality, to be classified as a less restricted Class I device.[58]

If, for example, the application is used to aid some other medical device, such as maintaining record of a diabetic patient's blood sugar levels as transmitted from the reader or imputed by the individual, then it could be regulated as class I.[59] In such an example, the app itself is neither analyzing the blood sample nor independently interpreting the results.[60]The application's sole functions are to aid

---

[53] *Id.* at 12, 16. ("This guidance does not address the approach for software that performs patient-specific analysis to aid or support clinical decision-making.")

[54] Notably excluded from the guidance are apps used as: medical reference or teaching aids, general health logs, aids for office billing and appointment transactions, apps not marketed to treat specific medical conditions, and apps that are limited to functioning as electronic or personal health record system. *See id*at 20–22, Appendix A – Examples of Mobile Apps that are NOT Medical Devices.

[55] Guidelines for Industry and Food and Drug Administration Staff, *supra* note 1,at 6, n. 3.For regulation purposes, accessories are considered extensions of the medical devices they modify. Accessories are regulated under the same classification of the medical device they are associated with. *Id.*

[56] 21 C.F.R. § 861.7(h) (1980) (defining the use, form, content, and placement of proper labeling).

[57] Guidance for Industry and Food and Drug Administration Staff, *supra* note1, at 13, 19.

[58] *Id.*

[59] *Id.* at 14.

[60] *See id.* The draft guidance drew a parallel between such devices and an "infusion pump stand" which does no more than aid in the use of the infusion pump. "A mobile medical app that simply supports the intended use of the regulated medical device could be classified as class I with design controls as part of the quality system requirements." Draft

the user in reading the results and maintain a log over a period of time for analysis by the treating physician.

A second category of mobile medical apps would be classified by the device with which they are associated if the app "extends the intended use of the connected medical device."[61] In contrast with the first category, theses apps are not passive storage devices, rather, these apps have an independent existence and function that impacts the use of the device, making the app an integral part of the device. The proposal itself describes these types of apps as analytical extensions of the medical device.[62] Returning to the example of the blood monitor, such an app would do more than store data by performing some sort of additional analysis, such as comparing trends or performing a more detailed analysis on the sugars in the blood. If an app were to perform in such a way, it would be nearly impossible to separate the app from the device itself.[63] For that reason, the app is classified as if it is an extension of the device.[64]

In the final section of the guidelines, the drafters addressed the problem of apps that function independently of any other medical device.[65] The standalone category includes both mobile apps and traditional desktop software.[66]This genre of devices is distinguished from traditional mobile medical apps because they have an independent function aside from aiding or extending the utility of a pre-existing device: these apps have the purpose of "performing patient-specific analysis and providing patient-specific diagnosis, or treatment recommendations."[67] Because this class of apps has a different level of complexity, it would be impossible to force them into the same category as the previously mentioned categories of

---

Guidance for Industry and Food and Drug Administration Staff; Mobile Medical Applications, 76 Fed. Reg. 43689-01 at 43689 (submitted July 21, 2011).

[61] Guidance for Industry and Food and Drug Administration Staff, *supra* note 1,at 14–15.

[62] *Id.*

[63] *Id.*

[64] *Id.*

[65] *Id.* at 15.

[66] Guidance for Industry and Food and Drug Administration Staff, *supra* note 1, at 15–16.

[67] *Id.* The guidelines propose that these applications should be categorized similarly to software on which they run or the device they modify. *Id.*

apps. If anything, this mirrors the distinction made between mobile apps as a whole and their medical device counterparts. These drastically different devices, though working towards similar ends, need to be judged on different scales before releasing them to the public.

F. FDA Regulations – Conclusion

As with any major technological change, the law has struggled to keep pace.[68] Credit needs to be given where it is due: the developers of mobile medical apps have done everything in their power to comply with current FDA regulations for medical devices, as well as implement and enforce their own standards beyond what is required by the FDA.[69] Credit also needs to be given to the FDA for preemptively addressing the potential health risks through the approval of guidance.[70]However, one major shortcoming of the guidance is that the FDA completely skirts the issue of privacy concerns.[71] As this technology continues to develop, the FDA will have to develop minimum standards of privacy protections for medical mobile apps, including requirements for passwords, firewalls, and other forms of internal security. As will be discussed in the next section, mobile medical apps threaten personal user information.[72]

III. PRIVACY CONCERNS

It cannot be denied that, through increased use of social media and smartphone technology, vast amounts of user data are now available on the Internet.[73] Many websites and search engines track and store user data and information through the use of "cookies."

---

[68] Lyria Bennett Moses, *Recurring Dilemmas: The Law's Race to Keep Up with Technological Change*, 2007 U. ILL. J. L. TECH. & POL'Y 239, 239 (2007).

[69] *See* Ravindranath, *supra* note 15.

[70] *See* Guidance for Industry and Food and Drug Administration Staff, *supra* note 1.

[71] *Id.*

[72] Notably, the FDA's Guidance does not address wireless safety considerations. *See id.*

[73] Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L.J. 617, 617-18 (2002).

Cookies are web programs designed to save specific information regarding individual users as they explore "the web."[74] Information stored ranges in detail and depth from which sections of a particular page the user visited, to more detailed information such as the "referring" website and where the user went after exiting the page.[75] More troubling, however, is that these programs also have the capability to record the specific Internet Protocol ("IP") addresses for the computer used to search the website, individual email addresses and passwords, and financial information such as credit card numbers and billing addresses.[76] Once stored, information may be used in a multitude of benign ways in regards to saving preferences, creating personalized advertisements, and in contacting the user with future information.[77] More unsettling is that secure storage of such information has proven to be insufficient at best.[78] In recent years, there have been multiple occasions where websites and other Internet systems have been hacked by outside users to access the sensitive data stored by companies.[79] Hackers typically seek information including credit card numbers and other personal identifiers, which leads to identity theft.[80]

A. Mobile Medicine and Privacy

In 2010-2011, concerns over online security peaked as security

---

[74] GEORGE B. DELTA & JEFFREY H. MATSUURA, THE LAW OF THE INTERNET§ 9.03 at 9-32.7 (3d ed. Supp. 2013) ("The cookie contains information about what Web pages the user views, what language the user speaks, and other information based on the selections made while visiting the site."). The authors explain that the depth of information known about an individual user by the website may depend on if the user is registered or not. If they are registered, then the website will have more access to their information.

[75] *Id*; *see also* DANA SHILLING, LAWYER'S DESK BOOK §28.10 at 28-48 (2005) (information saved can also include records of online purchases).

[76] *Id.*

[77] Blaine Kimrey & Bryan Clark, *Cyberprivacy and Digital Privacy Risks,* 29 COMM. LAW. 10, 10 (2012).

[78] *Id.*("In 2010, a large national health care company reported that it incurred costs in excess of $7 million for investigating the circumstances surrounding a missing portable disk drive, notifying its members, and offering credit monitoring and identity theft insurance").

[79] *Id.* at 11-14.

[80] *Id.* at 10.

loopholes, such as "backdoor access," came to the forefront.[81] In the midst of a flurry of complaints and embarrassing headlines, app developers admitted that they did little to protect sensitive user information such as account and personal names, credit card numbers, and IP addresses, which left users vulnerable to identity theft and credit card fraud.[82] In response, the FCC required increased security and required app builders to include internal protection within the application program itself.[83] The FCC reaction underscores the fact that apps are more than a harmless diversion. Potentially stored within the app is sensitive personal identifying or credit information.[84] This risk is enhanced when sensitive information regarding current or past medical history is added to the equation.[85]

An independent market for applications has been created for developers to address privacy concerns inherent in mobile apps while continuing to integrate them into the lives of patients, which

---

[81] In 2010 there were a number of examples of security breaches involving online data systems. *See* Niall Firth, *More than 114,000 Apple iPad Users Have email Addresses Exposed in Massive Hacking Attack*, THE DAILY MAIL,(June 10, 2010, 3:24 PM),http://www.dailymail.co.uk/sciencetech/article-1285505/Apple-iPad-security-breach-114-000-email-addresses-exposed.html#ixzz2I6TE6iTQ; Chris V. Nicholson and Eric Dash, *Citi Says Credit Card Customers' Data Was Hacked*, N.Y. TIMES(June 9, 2010, 12:49 PM),http://dealbook.nytimes.com/2011/06/09/citigroup-card-customers-data-hacked/.

[82] Hiroko Tabuchi, *Sony Freezes Gaming Accounts After Hacking Attack*, N.Y. TIMES(October 12, 2011),http://www.nytimes.com/2011/10/13/technology/sony-freezes-accounts-of-online-video-game-customers-after-hacking-attack.html.*See also* Nick Bilton & Brian Stelter, *Sony Says PlayStation Hacker Got Personal Data,* N.Y. TIMES,(April 26, 2011),http://www.nytimes.com/2011/04/27/technology/27playstation.html.

[83] Jordan Usdan et al., *FCC and Public-Private Partners Launch Smartphone Security Checker to Help Consumers Protect Mobile Devices This Holiday Season*, FCC OFFICIAL BLOG (Dec. 17, 2012), http://www.fcc.gov/blog/fcc-and-public-private-partners-launch-smartphone-security-checker-help-consumers-protect-mobil

[84] Giles Hogben & Marnix Dekker, *Smartphones: Information Security Risks, opportunities, and recommendations for Users,* ENSIA, 11 - 14 (Dec. 2010),*available at* http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/smartphones-information-security-risks-opportunities-and-recommendations-for-users.html.

[85] "If their habits and patterns deviate in a way that suggests they've become withdrawn, the app alerts a doctor or other caregiver to check in." Matt Richtel, *Apps Alert the Doctor When Trouble Looms*, N.Y. TIMES (Oct. 8, 2012 7:15 PM), *available at* http://well.blogs.nytimes.com/2012/10/08/apps-alert-the-doctor-when-trouble-looms/ (describing the new wave of mobile medical apps that transmit geo-location and activity logs to treating physicians or primary care givers).

limits the number of individuals who can use these types of apps.[86] While restricted access is beneficial, it fails to address what can be done to protect the user once the application is running on a mobile device, which is potentially transmitting private information.[87]

B. Electronic Health Records and Personal Health Records[88]

Ultimately, all mobile medical apps are a type of electronic medical record. Due to the variety of possible uses, concerns are specific to the capabilities of each individual app.

Electronic health records ("EHR") are the broadest category of digital medical records. The original function of the EHR was to streamline medical records within individual offices, and in particular to help make records more legible.[89] Therefore, EHRs are typically considered extensions of traditional paper records, securely

---

[86] Many companies such as Happtique, the National Center for Telehealth and Technology (T2), WellDoc, and others are preparing apps to be sold through their own platforms (called MRx in the case of Happtique). Dr. Greg Reger, *Smart Phones, Service Members &PTSD Treatments*, NAT'L CENTER FOR TELEHEALTH&TECH. ,*available at* http://t2health.org/print/454 (last visited Oct. 7, 2013). This is done on platforms like MRx where doctors are required to select ("prescribe") the application for their patient, and send it directly to their inbox. The patient themselves does not access the directory to select the app of their choice. Ravindranath, *supra* note 15.

[87] Winn, *supra* note 73, at 621-22.("Patients are highly sensitive to disclosure of their health information. The disclosure of certain types of adverse health information can have a powerful, often destructive, impact on the person who is the subject of that information. Many diseases have a social stigma that no laws against discrimination can banish. Even the disclosure of some medical conditions that are not contagious and have no adverse impact on others may damage an individual's reputation with colleagues, friends, and family . . . .The simple fact is that disclosure of such highly charged personal information can matter greatly to the affected person simply because that information is so intimate and so personal.")

[88] An electronic medical record is one kept in an online database and maintained for use by the treating physician. It is treated in the same way as a traditional medical record. A personal medical record is one maintained by the individual patient, and may be created and stored in any number of medium. In contrast, a patient portal is a similar online document where patients can go in and edit their EHR using a password, and their corrections become part of the medical record. Leslie P. Francis, *When Patient Interact with EHRS Problems of Privacy and Confidentiality*, 12 HOUS. J. HEALTH L. &POL'Y 171, 174-77 (2012).

[89] *Id.* at 171-72, 74.

stored in an office.[90]

Traditionally, there has not been a universal system where these records may be viewed or altered by multiple doctors. As a type of EHR, mobile medical apps have the potential to revolutionize the way medicine is practiced and will most greatly impact the patient who regularly visits multiple doctors or travels frequently for work.

Personal Health Records ("PHRs") are distinct from EHRs, in that the patient has direct control over the input into their medical record.[91] Because access is not restricted to medical professionals, PHRs are not granted the same level of protection as EHRs.[92] In that respect, mobile medical apps are comparable to PHRs. Many of these apps allow patients to enter daily symptoms or activities for later review.[93] Given the individualized nature of each disease, subjective patient control of medical records is ideal for long-term monitoring of chronic disorders.[94]

It is the precarious nature of data storage that makes security so important. The information patients record may range from the mundane (tracking pain or caloric intake) to the highly sensitive (monitoring HIV/AIDS or PTSD).[95] Many individuals living with highly personal and polarizing disorders, such as HIV/AIDS and PTSD, face social prejudice from inferences regarding their past, sexuality, or lifestyle.[96] Applications monitoring progressive disorders face the same potential risks as those monitoring psychological conditions, to be discussed below.[97]

---

[90] *Id.* at 182-83.

[91] *Personal Health Record: A Tool for Managing Your Health*, MAYO CLINIC (June 16, 2011), http://www.mayoclinic.com/health/personal-health-record/MY00665.

[92] *Id.*

[93] Brustein, *supra* note 23.

[94] *Id.*

[95] *Id.* The example given is of an app that will collect input about a "patient's diet, blood sugar levels and medication regimen." The application (Diabetes Manager) would then advise the individual on recommended foods based on blood sugar readings, as well as process, analyze, and send results to the treating physician.

[96] Winn, *supra* note 75, at 622.

[97] Brustein, *supra* note 23.

C. Psychological and Progressive Conditions

Apps concerning psychological and progressive conditions create a tangled morass of the need for access to hypersensitive information while preserving the delicate patient-doctor relationship.[98] Data stored, and potentially transmitted wirelessly, ranges from mundane entries made by the individual patient, to records of the patient's cellular usage patterns that a psychiatrist could use to monitor a patient with PTSD or manic-depressive bipolar disorder.[99] With most long-term conditions, trust and confidentiality are central to a healthy patient-physician relationship.[100] However, it is easy to see how a patient could feel that their doctor is prying into their private life, shifting the dynamic in the doctor-patient relationship.[101]

It has been suggested that these apps may also play the role of "surrogate" therapist.[102] For many doctors, time demands are on the rise.[103] There is an increase in the number of appointments booked throughout the day, and there are very real limitations on an individual doctor's physical resources.[104] It is hoped that apps will

---

[98] One risk, not addressed in this paper, is that of patients who could potentially use such an app as a way to blur the line between doctor and patient and no longer rely on their physician. Katie Hafner, *Redefining Medicine with Apps and iPads,* N.Y. TIMES, Oct. 8, 2012, at D1, *available at* http://www.nytimes.com/2012/10/09/science/redefining-medicine-with-apps-and-ipads-the-digital-doctor.html.

[99] The mildest app thus far will remind users when to take their medications daily. A more advanced version of the app will notify physicians if the medicine bottle is not opened daily. Krouse, *supra* note 14, at 740.

[100] Winn, *supra* note 73, at 622 ("The dangers associated with disclosure of personal health information have a strong practical impact on the relationship of trust between a patient and a physician.").

[101] Perhaps the greatest, but least obvious, victim of the use of mobile medical apps is the degradation of the physician-patient relationship. As patients rely more heavily on mobile medical apps, it may distance the patient from their doctors. As doctors monitor from a distance, patients may perceive their doctor's interception of information as spying or prying and withdraw their trust.

[102] Elizabeth Landau, *Smartphone Apps Become 'Surrogate Therapists,'* CNN (Sept. 27, 2012, 12:21 PM), http://www.cnn.com/2012/09/27/health/mental-health-apps/index.html.

[103] *Seeid*.; CTR. FOR WORKFORCE STUDIES, RECENT STUDIES AND REPORTS ON PHYSICIAN SHORTAGES IN THE US (2012).

[104] *See* Landau, *supra* note 102; Ctr. for Workplace Studies, *supra* note 103.

play the role of a "temporary therapist" to help with daily exercises or minor behavioral adjustments.[105]One example includes a behavioral modification app directed towards individuals living with OCD.[106] While physician time is a finite commodity, the ethics of such an app are in question as it facilitates the degradation of the doctor-patient relationship as reliance is placed on the device.[107]

IV. INTERNET, PRIVACY, AND MOBILE MEDICINE [108]

Mobile apps are susceptible to the same security concerns as websites and other Internet accessible devices.[109] Extraneous data collected from cellphones includes geographic location (as the device "pings" off of the nearest cellphone tower), records of access to and activity within specific apps, and use of the cell phone's internal address book.[110] Because most purchases of apps are paperless, credit

---

[105] Landau, *supra* note 102.*Butsee*, Richard A. Friedman, *Recalibrating Therapy for Our Wired World*, N.Y. TIMES, Oct. 8, 2012, at D6, *available at* http://www.nytimes.com/2012/10/09/health/recalibrating-therapy-for-a-wired-world-the-digital-doctor.html.

[106] Landau, *supra* note 102("The technique forces patients to face their fears head-on without engaging in compulsions. Users can practice this with, for instance, leaving the house without checking the door lock multiple times, over a given time period. If they give in before the timer is up, there's a 'Just Gave In' button.").

[107] Friedman, *supra* note 105.

[108] In addition to privacy and security issues, a debate has sparked surrounding cellphones, apps, and the Fourth Amendment. S*ee* J. Patrick Warfield, Note, *Putting a Square Peg in a Round Hole: The Search-Incident-to-Arrest Exception and Cellular Phones,* 34 AM. J. TRIAL ADVOC. 165 (2010); Daniel Zamani, Note, *There's an Amendment for That: A Comprehensive Application of Fourth Amendment Jurisprudence to Smart Phones,* 38 HASTINGS CONST. L.Q. 169 (2010); Leanne Andersen, Article, People v. Diaz*: Warrantless Searches of Cellular Phones, Stretching the Search Incident to Arrest Doctrine Beyond the Breaking Point,* 39 W. ST. U. L. REV. 33 (2011).

[109] *See* Kimrey & Clark, *supra* note 77.; *see also* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461 (2000).

[110] THE PRIVACY RIGHTS CLEARING HOUSE, *What is your Smartphone Capable of Revealing About You?*(Aug. 2005), https://www.privacyrights.org/fs/fs2b-cellprivacy.htm#smartphonedata (stating smartphone service providers collect information including: incoming and outgoing calls and text messages, phone numbers users communicate with, how often users access the Internet and user's location).

card and pin numbers may be linked to a specific electronic device.[111] On a base level, there are questions about what can be done to secure a user's private credit information, and the contact information of their friends, family, and colleagues.[112] Newer devices have the capability to track a user's geographic location in their home, and their location throughout the course of their day.[113]

Proposed mobile medical apps poised to hit the market will record far more than places of interest on a website and geographic location. As previously mentioned, some of the newer apps will transmit information directly from the device to the treating physician.[114] This new genre of medical records has the capability to amass large amounts of information in a short amount of time, tracking everything from the most mundane to the most intimate aspects of an individual's life.[115] The app's ability to record vast amounts of patient information in a short amount of time distinguishes it from a traditional medical record that sits stationary in a doctor's office and contains a mere "snapshot" of an individual's medical history.[116]

Once connected to the Internet, records are open to a wider variety of threats such as hacking[117] Should that occur, the user loses more than identification and financial information.[118] Any semblance of privacy is shattered.[119] Particularly surrounding sensitive conditions that the patient would want kept private, there is a great

---

[111] Daniel L. Pieringer, Recent Development, *There's No App for That: Protecting Users from Mobile Service Providers and Developers of Location-Based Applications,* 2012 U. ILL. J.L. TECH. & POL'Y 559, 565 (2012).

[112] Paul Ruggiero & Jon Foote, *Cyber Threats to Mobile Phones,* U.S. COMPUTER EMERGENCY READINESS TEAM, 1, 3-4, (2011), http://www.us-cert.gov/reading_room/cyber_threats_to_mobile_phones.pdf.

[113] *Id.* at 3.

[114] Landau, *supra* note 102; Ravindranath, *supra* note 15; Brustein, *supra* note 23.

[115] Winn, *supra* note 73, at 621.

[116] *See* TOPOL, *supra* note 14, at 60.

[117] Winn, *supra* note 73 at 617-18.

[118] *Id.* at 621.

[119] *Id.*

risk of embarrassment upon discovery or revelation.[120]

Because most smartphones can be "unlocked" with the swipe of a finger, additional concerns arise regarding ease of access to apps. Many apps continue to run in the background of the device even when they are not currently in use.[121] Even then, most do not require a login to reopen the program every time it is closed.[122] Access to an app is but a tap away for the curious snoop. The gist of the mobile medical app discussion is that mobile apps occupy a sort of grey area between what can be protected, and what is unprotected.

A. HIPAA and Mobile Medical Technology

In 1996 Congress addressed the problem of protecting patient privacy by passing the Health Insurance Portability and Accountability Act of 1996 (commonly known as "HIPAA").[123]Central to the Act is a provision known as the Privacy Rule, which regulates the "use and disclosure of individuals' health information" by those entities covered under the Act.[124] It also guides health care providers (as "covered entities") on how to handle and protect individual information.[125]HIPAA, through the Privacy Rule, attempts to strike a delicate balance between the free flow of information necessary to

---

[120] *Id.*

[121] *How to Completely Close Out Running Applications in the New iPhone iOS 4*, WONDERHOWTO.com(2013),http://smartphones.wonderhowto.com/how-to/completely-close-out-running-applications-new-iPhone-ios-4-377560/.

[122] *Id.*

[123] *Summary of the HIPAA Privacy Rule*, USDHHS AND OFFICE FOR CIVIL RIGHTS,http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf (last updated May 2003); Health Insurance Portability and Accountability Act, 29 U.S.C. §§1181-83 (1996).

[124] Health Insurance Portability and Accountability Act, 45 C.F.R. § 164.502 (2002) (sets the standard that "A covered entity may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter."); Health Insurance Portability and Accountability Act, 45 C.F.R. § 160.103 (2012) ("Covered entity means: (1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter."); *see also* Summary of the HIPAA Privacy Rule, USDHHS AND OFFICE FOR CIVIL RIGHTS (May 2003), *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf

[125] Health Insurance Portability and Accountability Act, 45 C.F.R. § 164.510 (2011); *see also* Summary of the HIPAA Privacy Rule, *supra* note 126, at 1.

treat a patient and the right to privacy and security that is due every individual.[126]

The HIPAA Privacy Rule ultimately protects all "individually identifiable health information" that may be recorded, transmitted, or stored by healthcare providers.[127] Under the Act, "protected health information" is defined as information that can be used to "personally identify" an individual patient, unless it is being used for certain, specified reasons.[128] As defined by statute, this subset of information includes common identifiers such as name, contact information, geographic location, or race; past or present health history; and any other data that could reasonably identify the individual patient.[129] However, under the "safe harbor" provision, when those personal identifiers are removed, all restrictions are lifted.[130] This protects researchers and aids the Department of Health and Human Services investigate practitioners' habits. At least this general definition seems to fit what will be stored in mobile medical apps: personal identifying information. However, HIPAA governs what covered entities do, not what becomes of personal information once it leaves the covered entities' control.

To protect the patient, covered entities must limit the collected data to the "minimum necessary to accomplish the intended purpose of the use, disclosure, or request."[131]Covered entities must also limit access and use of that information.[132] This poses another hurdle to the reconciliation of mobile apps with HIPAA, because these devices often gather surplus information that is not directly necessary for treatment. As previously mentioned, apps track everything from usage and geo-location, to personal identifiers.

As technology evolved, PHRs (in the form of online databases) developed to store medical records. These web pages were protected

---

[126] SUMMARY OF THE HIPAA PRIVACY RULE, *supra* note 126, at 1.

[127] SUMMARY OF THE HIPAA PRIVACY RULE, *supra* note 126, at 3.

[128] Health Insurance Portability and Accountability Act, 45 C.F.R. § 160.103 (2006).

[129] *Id.*

[130] Health Insurance Portability and Accountability Act, 45 C.F.R. § 164.502(d)(2) (2002); Health Insurance Portability and Accountability Act, 45 C.F.R. §§ 164.514(a)- (b) (2002).

[131] Health Insurance Portability and Accountability Act, 45 C.F.R. § 164.502(b) (2013).

[132] Health Insurance Portability and Accountability Act, 45 C.F.R. § 164.514(d)(1) (2013).

through a user specific log in, and generally could only be edited by the treating physician.[133] In that sense, the documents retained the protection they would have had if they had been kept in the office.[134] However, once the document was downloaded onto the user's computer, it was no longer covered by HIPAA.[135] The question remains: As technology of this nature continues to evolve, how can a patient's personal information be protected?

B. HITECH and Beyond: What Remedies Other Areas of Law Offer

While HIPAA seeks to be "flexible and comprehensive," one problem is that it was written and enacted long before much of modern technology was developed. It is obvious that, as written, HIPAA does not extend to mobile medical apps. It seems as though the objective to protect patients must live on in some other area of law. Another major problem is that HIPAA left patients without an individual cause of action against practitioners who did not follow the prescribed guidelines.[136]

In 2009, President Barack Obama signed into law the American Recovery and Reinvestment Act, which contained a provision called the Health Information Technology for Economic and Clinical Health Act (commonly HITECH) that expanded and updated key HIPAA provisions.[137] These included: updating the notification requirements; expanding the liability for business associates; and creating a class action option for patients whose information had not been securely protected.[138]

The option for class action should not be the end of the story. The ever-evolving development of the Internet and mobile technology

---

[133] *See* Francis, *supra* note 88, at 174, 177-78.

[134] *See id.* at 177-78.

[135] *Id.* at 178.

[136] Scott L. Vernick& Amy C. Purcell, *The HITECH Act*, 1 DATA SECURITY& PRIVACY L. § 7:29 (2013).

[137] *See generally* American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115; Vernick & Purcell, *supra* note 136.

[138] *See id.*(Although the HITECH Act does not permit a private cause of action, a state attorney general may institute an action on behalf of the state's residents.).

has continually outpaced legal development.[139] Some legal commentators encourage looking beyond the parameters of a specific area of the law in order to find answers.[140] In the last fifteen years, Internet privacy law has expanded by leaps and bounds.[141]There are two major challenges to applying Internet privacy law to health law: (1) the laws and regulations surrounding Internet privacy are highly technical; and (2) there is no universal code.[142] Despite these obstacles, it is possible to apply the principles of Internet privacy law to the burgeoning mobile medical app market.

Beginning in 1996, legislation governing the interception of wire and electronic communications became effective.[143] These provisions are known commonly as the Electronic Communications Protection Act (ECPA).[144] Sections of the ECPA incorporate provisions of the Wiretap Act.[145] The act is designed to protect electronic communications as they are stored or transmitted.[146] In 2003, individual users sued five pharmaceutical companies (American Home Products Corporation, Glaxo Wellcome Incorporated, Pfizer Incorporated, Pharmacia Corporation and SmithKline Beecham Corporation)and a separate corporation that was tracking personal information, Pharmatrack.[147] The First Circuit laid out a five-part test for an individual seeking the protection of the ECPA:

---

[139] *Cf.* Natasha Singer, *Technology Outpaces Privacy (Yet Again)*, N. Y. TIMES(Dec. 11, 2010),http://www.nytimes.com/2010/12/12/business/12stream.html.

[140] McEnery, *supra* note 2, at 19.

[141] Timothy J. Toohey, *Piracy, Privacy, and Internet Openness: The Changing Face of Cyberspace Law,* in UNDERSTANDING DEVELOPMENTS IN CYBERSPACE LAW, 97 (2012), *available at* 2012 WL 2244536.

[142] *Id.* ("Complicating matters is that cyberspace law is not only a relatively technical field, but is also not always easy to locate. It is not embodied in any one legal code, but is instead scattered over many state and federal laws.").

[143] 18 U.S.C. §§ 2510-22 (2006 & Supp. 2011).

[144] *Id.*

[145] Electronic Communications Protection Act of 1968, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. 119 (1986)).

[146] 18 U.S.C. §§ 2510-11 (2006) (defining "electronic communication" and prohibiting the "interception and disclosure of wire, oral, or electronic communications"); 18 U.S.C. §2701 (prohibiting "unlawful access to stored communications").

[147] *In re Pharmatrack, Inc.,* 329 F.3d. 9, 15-16 (1st Cir. 2003).

> . . .that a defendant (1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication (5) using a device. This showing is subject to certain statutory exceptions, such as consent.[148]

The court highlighted that "'contents,' when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication."[149] In addition, it is emphasized that patient names, birth dates, and medical condition are protected under the act as personal identifying information.[150]Looking at how the court applied the statutory provision in 18 U.S.C. §2511(a), it seems as though this provision could be extended to protect patients should their information be intercepted as it is transmitted to their doctor. This is especially true in cases where the app is going beyond record keeping by conducting in-depth analysis or creating charts.

Transmissions are not the only data covered by the ECPA. Stored communications and data may not be accessed intentionally without the express authorization of the user or entity storing it.[151]Possible punishment includes a fine levied against the hacker, or up to five years imprisonment.[152] This provision of the ECPA would seem to protect the data collected about the individual patient while it is stored in the application.

Finally, the ECPA gives aggrieved individuals a civil remedy against any person (or company) that accesses personal information as it is transmitted or stored.[153] This provision authorizes:(1) actual damages; (2) additional or punitive damages, in certain situations; and (3) reasonable attorneys' fees or litigation costs when incurred.[154] Should the ECPA extend to medical apps, this act would provide the

---

[148] *Id.* at 18.

[149] *Id.* (citing 18 U.S.C. §2510(8) (effective Nov. 2, 2002)).

[150] *Id.* (citing Gelbard v. U.S., 408 U.S. 41, 51 n.10 (1972)). *See also* 18 U.S.C. §2510(12) (2006) (including "data" in definition of "electronic communication").

[151] 18 U.S.C. §2701(a) (2006).

[152] *Id.* at §2701(b).

[153] 18 U.S.C. §2520(a) (2006) (authorizing civil damages for victims).

[154] *Id.* at § 2520(b).

patient with an individual cause of action against the party who inappropriately accessed their information. In conjunction with HITECH's authorization of a class remedy against the covered entity that improperly discloses data, this act could allow the patient to have full recovery against both their doctor and their perpetrator.[155]

Even though HITECH and ECPA do not extend to mobile medical apps, they should be used as a starting place when drafting guidance and legislation addressing privacy concerns raised by such programs. First and foremost, Congress should permit an individual cause of action for patients whose information is intercepted or accessed without their consent against the individual hacker, echoing the ECPA. This way the actual perpetrator of the privacy violation is held accountable for the harm he causes the user. Drawing from HITECH, Congress should permit class action suits against developers of medical apps who do not implement sufficient safeguards. A class action option is appropriate because it restricts the amount of litigation developers are exposed to, and limits litigation to widespread defects in the program rather than localized glitches.

While an individual cause of action would benefit potential users of medical mobile apps, there are many challenges that will have to be addressed. For example, at least one court has held that the ECPA does not cover civil procurement or agency theories of liability.[156] Under that holding, if an individual hires someone to intercept an electronic communication they cannot be held liable under the act (the principal), but the person who actually intercepted the communication (the agent) may be.[157] This flips basic agency theory on its head, which traditionally holds the principal liable for the actions of the agent within the scope of his employment. The court also held that the principal in such a situation could not be held liable under theories of conspiracy or aiding and abetting.[158]

Congress has an opportunity to draft legislation echoing the ECPA while circumventing its shortcomings. There is a tension in the

---

[155] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat 115 (2009).

[156] *Shelfts v. Petrakis*, No. 10–cv–1104, 2013 WL 3187971, at *4 (C.D. Ill.June 21, 2013).

[157] *Id.*

[158] *Id.*

ECPA because the act creates an individual cause of action against perpetrators who intercept electronic communications, but prevents liability based on agency theory, conspiracy, and aiding and abetting. By carefully drafting legislation to include liability based on agency and party theories, a culpable principal would not be able to shield itself behind a judgment proof agent. That risk is a real possibility when the principal is a company with assets that could be seized to satisfy a judgment. While civil or criminal sanctions can hardly help a victimized individual regain their sense of privacy or security, financial penalties and criminal sanctions will act as a deterrent towards other potential perpetrators.

Creating a class remedy against developers would serve a dual purpose of protecting the interests of the researchers while giving the injured user recourse. By requiring plaintiffs to satisfy class requirements, developers will have the freedom they need to develop an innovative product without the risk of a deluge of litigation, so long as care is taken to safeguard user information. Liability can be limited to problems in the program itself, excluding glitches that are attributable to other forces like unsecure Internet connections. However, the possibility of class action would be a check to make sure that developers are not taking risky shortcuts. It will also give the injured user the possibility of financial recourse from the developer.[159]

Additionally, Congress should consider distinguishing between information intercepted while it is being transmitted from the app to a treating physician versus stored information that is accessed without the user's consent.[160] In the former situation, intercepting transmitted information opens a hacker to a civil action for the first offense, and a civil fine the second.[161]

However, for accessing stored information, a perpetrator is subject to criminal liability; including fines and jail time on the first

---

[159] But, it has been argued that class action lawsuits are inadequate to compensate injured plaintiffs because it is uncertain whether they will receive any meaningful compensation. *See* Alexander B. McLean & Thomas R. McLean, *Dependence on Cyberscribes–Issues in E-Security*, 8 J. BUS. & TECH. L. 59, 94 n.272 (2013).

[160] 18 U.S.C. §§ 2511, 2701(a) (2006).

[161] 18 U.S.C. § 2701(b) (1)-(2) (2006).

offense.[162] Congress should consider a similar construction for creating a certain civil penalty and the potential for criminal liability. Doing so would offer immediate recourse to injured patients while offering additional deterrence against hacking into medical apps.

V. CONCLUSION

Astounding progress has been made over the last 30 years in terms of medical and personal technology. In the past decade, smartphones have truly revolutionized the way we live. In that same timeframe, we have grown more conscientious of the dramatic increase in the diagnoses of chronic illnesses in our country.[163] Physicians latched on to cellular technology that has integrated itself so deeply into our lives in an attempt to utilize it as a tool for health monitoring, and eventually lifestyle change.[164] Through the development of mobile medical apps, it is hoped that healthier habits can be formed, and that, at a minimum, the user becomes more aware of the daily habits that impact their overall health.[165] Developers are vastly limited under the law as it currently stands. Guidance from the FDA is still new and only stands to prevent physical harm.[166] Even though HIPAA does much to protect patients, new technological advances have outpaced many of its protections. Concerns over personal information increases as mobile medical apps continue to develop. The risk of hacking opens up the user to the potential risk of

---

[162] 18 U.S.C. § 2701(b) (2006).

[163] PARTNERSHIP TO FIGHT CHRONIC DISEASE, *The Growing Crisis of Chronic Disease in the United States*, http://www.fightchronicdisease.org/sites/fightchronicdisease.org/files/docs/GrowingCrisisofChronicDiseaseintheUSfactsheet_81009.pdf (last visited Oct. 30, 2013).

[164] PAN AMERICAN HEALTH ORGANIZATION, *The Role of eHealth in the Prevention of Childhood Obesity*, http://new.paho.org/ict4health/index.php?option=com_content&view=article&id=62%3Athe-role-of-ehealth-in-the-prevention-of-childhood-obesity&catid=14%3Aarticulos&Itemid=44&lang=en; *see also*: APPLICATIONS FOR GOOD, *Mobile Health Apps for Low Socio-Economic Communities*, http://www.slideshare.net/applicationsforgood/mobile-health-apps-for-low-income-communities (last visited Oct. 18,_2013)

[165] Brustein, *supra* note 23.

[166] Guidance for Industry and Food and Drug Administration Staff, *supra* note 1.

identity or credit card theft, embarrassment, and social stigma should their sensitive health information be discovered.[167] One way to stay ahead of the risk is to look beyond the realm of health law to areas such as Internet privacy law.[168]

Acts, like the ECPA, provide for an individual cause of action by the injured plaintiff. While the ECPA provides a good starting place for drafting guidance specific to privacy concerns with mobile apps, it cannot be the stopping place. In order to offer proper recourse to harmed users, individual causes of action must be able to be brought against the actual person who wrongfully accessed the user's information, or who caused it to be wrongfully accessed. Also, Congress should consider how HITECH has expanded HIPAA through the inclusion of a class action option. By ensuring that users of mobile medical apps have individual and class recourse, a balance will be created that will allow this type of technology to evolve while allowing important checks on how the individual patients are protected.

[167] Winn, *supra* note 73.