THE REVIEW OF
MEDICAL INFORMATION MANAGEMENT
FOR LITIGATION

MIM REPORTER

SEPTEMBER 2015 EDITION

Published by Litigation Management, Inc.

Elizabeth B. Juliano
Founder & Chief Executive Officer
ebj@lmiweb.com
440.484.2001

What's New at LMI

- LMI was pleased to participate in the Hermes Cleveland Corporate Challenge 2015, a corporate athletic competition promoting company camaraderie, employee wellness and business networking while helping local charities. LMI has been participating in the Challenge since 2009. In the 2015 competition, LMI placed 3rd in the 3V3 Basketball competition for the Independent Division. Congratulations to Matt Gingrich, Charmiece Pinckney and Anthony Hollins!

- LMI employees Rebecca Bishop, Amy Kec, Charmiece Pinckney, Amber Mishler and Brooke Wolfe, working in partnership with BVU: The Center for Nonprofit Excellence, will be serving as pro bono consultants for Coach Sam's Inner Circle Foundation, a non-profit organization that provides Cleveland's inner city youth with opportunities that change lives and create an environment of positive mentored success. The project will involve analysis of the current local and national elementary non-profit programs offered in Cleveland, with a focus on curriculum scope and design, sources of funding, gaps in the community, and opportunities for collaboration.

- LMI is proud to announce its Gold-Level Corporate Partnership with the Sports & Fitness Industry Association (SFIA), the trade association of leading industry sports and fitness brands, suppliers, retailers and partners. SFIA supports member companies and promotes a healthy environment for the sporting goods industry by providing access to thought leadership, industry & public affairs, research and member services. SFIA enhances industry vitality and fosters sports, fitness and active lifestyle participation. *(cont. p2)*

Litigation Management, Inc.
6000 Parkland Boulevard, Mayfield Heights, Ohio 44124 | 800-778-5424 (ph) 440-484-2020 (fax)
Published as an educational service to the Corporate, Insurance and Defense Legal Community.
www.lmiweb.com

What's New at LMI (cont.)

- LMI Founder and CEO Elizabeth (Betsy) Juliano will be co-presenting an industry breakout session at the 2015 Fall Conference of the Product Liability Advisory Council (PLAC). The session, co-presented with Rita McConnell of Medtronic, will focus on hot topics in the pharmaceutical and medical device industries and will feature an in-depth look at the impact of electronic health records (EHRs) on injury-related claims and litigation.

Mobile Medical Apps & Wearable Devices: You Wear[able] it Well

Sci-fi movies and television shows of the past have featured "scanning" devices that assess one's vital signs, similar to Star Trek's tricorder device of the 1960s, or that scene in the 1990s movie Total Recall. Fast forward to present day where, over the past year, public interest in wearable computing technologies has grown significantly, primarily due to the introduction of Google Glass and a number of fitness trackers into the market, as well as the increasing promise of "smart watches" (including Apple's recent release of the much-anticipated iWatch). In fact, in 2014 alone, over 70 million fitness trackers were sold in the U.S.[i] That number will jump to a projected 90 million wearable devices in 2015.[ii]

A relatively new term, "The Internet of Things (IoT)," is now widely used to describe the incorporation of connectivity into one's offline life through devices such as wearables. "Wearables" (also known as wearable computers, wearable technology, or body-borne computers) are miniature electronic devices that are worn by the bearer, with or on top of clothing, for the purpose of tracking information, such as health and fitness. Wearable technology tends to be more sophisticated than hand-held technology because it can provide sensory and scanning features not typically seen in mobile and laptop devices, such as biofeedback and tracking of physiological function. Examples include: watches, glasses, contact lenses, e-textiles and smart fabrics, headbands, beanies and caps, and jewelry (such as rings, bracelets, and hearing-aid devices that are designed to look like earrings). By their very nature, "wearables" tend to refer to items which can be put on or taken off with ease, although there are more invasive versions of the concept, such as implantable microchips and even smart tattoos.

E-textiles? Smart tattoos? Believe it or not, yes.

Wearables are used for a wide range of purposes, but are typically used for health and fitness applications, such as tracking one's heart rate, body temperature, sleeping patterns, speed, and distances traveled while exercising. Currently, wearables are almost exclusively used by individuals, but many believe that the use of wearables will eventually spread to healthcare systems and businesses that want to monitor and track different activities, as well as provide incentives for their employees to stay healthy.[iii] In the future, wearables, along with the apps and services that come with them, could change the way workers do their day-to-day jobs and how consumers manage their private lives.

In fact, in a recent interview on NPR's *Morning Edition*, host Renee Montagne interviewed *Financial Times* reporter Sarah O'Connor about the benefits and pitfalls of using wearable technology

in the workplace, as more and more employers are showing an interest in collecting wearable data from their employees.[iv] (Ms. O'Connor, who had agreed to wear several devices for one week and share the results with her boss, summed up her thoughts at the conclusion of the interview: "I took [the devices] off on Friday night. It was an incredibly good feeling. I really grew to sort of hate them by the end, actually.")

As wearable devices and mobile medical apps gain popularity, it becomes increasingly important for manufacturers, developers, and legal practitioners to consider the myriad issues that will inevitably arise as a result of this rapidly expanding technology.

There is an increasing level of attention on the potential privacy issues and concerns, from a user perspective, an employee perspective, and even a corporate perspective. Individuals are unsure what data is being collected by third parties and how such data is being used. Employees are concerned that employers may use data against them from an insurance, wellness, or even employability perspective. Companies are not only faced with potential patent issues, but are also concerned that data breaches could open them up to liability claims, or that data could be used in corporate espionage.

Consider the following questions:

- What other impact might wearables and medical apps have on the legal industry?
- How can the data be used in litigation, whether it be a personal injury claim (like a car accident or worker's compensation, where the device may contain relevant evidence), or in a product liability action against a device manufacturer (where a plaintiff alleges a wearable device actually caused him or her medical injury)?
- Is data from wearable devices accessible outside of proprietary software?

Section II ("Litigation Considerations") will provide general insight and practical considerations for manufacturers, developers and legal counsel. First, however, one must first have a general understanding of the regulatory scheme surrounding these products.

I. Regulatory Background

In early 2015, the Food & Drug Administration (FDA) issued draft guidance relating to the oversight of general wellness products (including wearable health-related devices), health IT, and medical device accessories.[v]

Fitness and wellness tracking devices are generally defined as promoting overall wellness, having no claims to solving specific medical conditions, and relatively safe to use.[vi] The FDA appears to be taking a largely hands-off stance to these devices, claiming that the low risk to consumers does not currently require government oversight. Included within the application of this definition is the popular Fitbit® fitness tracking bracelet.[vii] Bakul Patel, the FDA's associate director for digital health, stated in a recent interview, "we are taking a very light touch, an almost hands-off approach…If you have technology that's going to motivate a person to stay healthy, that's not something we want to be engaged in." [viii]

What remains less clear, however, is how the FDA plans to address wearables that function more like a medical device, by way of tracking or making more explicit medical claims regarding the treatment of a specific disease or illness.[ix] Although the FDA is apparently intending to monitor technologies that aim to diagnose illnesses or even recommend treatment options, there are unresolved issues as to the level of scrutiny required. For example, in the draft guidance, the FDA suggests that newly created medical device "accessories" may not necessarily be subject to the stringent regulation and approval process that "regular" devices follow.[x] According to the agency, "classifying an accessory in the same class as its parent device is appropriate when the accessory, when used as intended, meets the criteria for placement in that class. However, some accessories can have a lower risk profile than that of their parent device and, therefore, may warrant being regulated in a lower class." [xi]

While the FDA may not be closely monitoring wellness devices and technology, other federal agencies are taking an interest in these products, especially where the products have caused post-market consumer concerns. For example, the U.S. Health and Human Services Office of Civil Rights is scrutinizing the impact of patient-health data that is being collected by wearables and other devices, while the Federal Trade Commission (FTC) has cracked down on technology that dubiously claimed to assess and detect the risk of melanoma by analyzing an uploaded image of a skin lesion.[xii] Additionally, the Federal Communications Commission (FCC) recently announced the formation of a new Commission Task Force to "bring together the expertise of the FCC on the critical intersection of broadband, advanced technology, and health" (CONNECT2HEALTHFCC).[xiii]

In the November/December 2014 issue of the Food & Drug Law Institute (FDLI) *Update* magazine, Shook Hardy & Bacon LLP attorneys described the "complicated regulatory landscape with overlapping agencies eyeing the risks that these new devices could pose to users."[xiv] Concluding that "[m]obile medical applications are a new frontier

that government agencies are only just beginning to address," the authors caution developers to gain "a clear understanding" of applicable regulations and agency expectations to successfully navigate any potential risks in bringing these products to market.

II. Litigation Considerations

Privacy & Liability

In the wearable fitness and health device industry, technology is advancing faster than the development of laws and regulations. As mobile health ("mHealth") and wearable device capabilities increase, questions remain as to whether manufacturers and developers are taking prudent steps to protect personal health data privacy, stop data from being sold to third parties, and secure against hacking.

It is not entirely clear whether HIPAA will apply to wearable manufacturers and developers, as HIPAA is intended to govern electronically transmitted data in connection with specifically defined transactions (such as the submission of health claims to a health insurer).[xv] For example, if a device will be collecting protected health information (PHI), but the data will not be shared with a covered entity, then HIPAA may not be applicable. Nonetheless, state privacy and security laws (which often mirror HIPAA language) may very well still have implications.[xvi] It is therefore very important for manufacturers and developers to have a full understanding of applicable privacy and security laws in order to assess what, if any, provisions will be applicable to their specific technology. Developers and manufacturers should also consider employing increased information security measures, which are further discussed below (see section III, "Preventive Measures and Best Practices").

Consider also the impact on healthcare providers who recommend the use of mobile health and fitness apps or devices to their patients. "By recommending apps that compromise patients' privacy, doctors could be seen as complicit if there is any breach, although there is no apparent legal precedent for that."[xvii] At least, not yet. It may be prudent for healthcare providers to consider the type of data being collected, as well as the data management practices of the service provider(s), and advise their patients of the potential privacy and security risks so the patient can make an informed choice about the use of the device.

Product Liability

In September of 2014, the *Medicine & Science in Sports & Exercise* journal published the results of a study performed by researchers at Iowa State University, testing the accuracy of wearable fitness trackers, such as the Fitbit®, Nike+ FuelBand, and BodyMedia FIT.[xviii] Remarkably, the study found

"By recommending apps that compromise patients' privacy, doctors could be seen as complicit if there is any breach, although there is no apparent legal precedent for that."

the tested wearable fitness trackers to be between 15 to 40% inaccurate in tracking user activity.

Consumer Reports recently tested several wireless blood pressure monitors and blood glucose meters, finding at least two blood pressure monitors reflecting accuracy issues, as well as a number of complications that made using blood glucose meters challenging to wearers.[xix] Although the average scores of the tested meters complied with the FDA's requirement of accuracy within 15%, *Consumer Reports* noted that the tested models still needed some work.

This presents a number of concerns from a product liability perspective, perhaps the most obvious being: Who is liable if the end user is injured? Similar to many product liability claims, the supply chain can present some complications in determining liability. If the product was being used at the direction or under the care of a medical professional, it is likely that both the medical professional and the manufacturer (and/or developer) would be sued if use of the app or device lead to injury or death.[XX]

In the specific context of wearable technology, not only could the manufacturer and/or developer be the subject of litigation, but co-developers and even marketplace hosts (such as the Apple "App Store") and carriers (such as Verizon or Sprint) could theoretically be parties to product liability claims.[xxi] Although many state legislatures have imposed caps on non-economic damages against healthcare providers, such caps are not common for wearable device manufacturers.[xxii] For developers, manufacturers, marketplace hosts, and carriers, disclaimers and user agreements could become a critical tool in shielding at least some of the potential liability concerns.

For now, product liability in the context of wearables and apps is largely unchartered territory, still awaiting scrutiny by juries, judges and lawmakers. However, it is likely that once a few claims are filed, there could be a veritable "opening of the floodgates," with manufacturers (and, of course, their legal counsel) scrambling to find solid legal ground.

Using Wearable Data in Discovery

"Self-tracking using a wearable device can be fascinating. It can drive you to exercise more, make you reflect on how much (or little) you sleep, and help you detect patterns in your mood over time. But something else is happening when you use a wearable device, something that is less immediately apparent: You are no longer the only source of data about yourself. The data you unconsciously produce by going about your day is being stored over time by one or several entities. And now it could be used against you in court." [xxiii]

The above statements were made following the first known court case involving wearable device data. A law firm in Calgary is using data from a Fitbit® device

in a personal injury claim to show that the plaintiff, a personal trainer, experienced reduced activity levels as a result of the alleged injury at issue. The case presents several unique matters for consideration, such as how best to collect, analyze or use data from wearable technology.

Fitbit® and other wearable data often involve complex algorithms, storage methods, and even interaction with multiple devices, apps, or data sources. Collection can be complicated and the data will almost certainly not appear in a friendly, searchable Word document format. This will inevitably present review and analysis complications. The attorneys in the Calgary case are using a somewhat novel approach by relying on an analytics company, Vivametrica, to synthesize the data. The plaintiff's results were then compared to "average" population fitness and activity levels, thereby demonstrating that the plaintiff was significantly below baseline levels for someone in her age range and profession.

In cases involving wearable devices, it will be important to fully understand the manner in which data is collected, stored, transmitted, and analyzed by applicable algorithms. Attorneys will need to determine where data is being stored (which will often be in multiple locations), as well as ensure that any resulting evidence can be authenticated. Because wearables can be removed, or (in many cases) worn by another individual altogether, reliability and chain of custody may also be an issue.

III. Preventive Measures & Best Practices

As technology rapidly advances, there are a number of preventive measures and best practices that device manufacturers and developers (and their legal counsel) can put into place to alleviate some of the potential privacy, liability and data accessibility concerns.

In November of 2013, the FTC hosted a workshop entitled *The Internet of Things: Privacy and Security in Connected World.*[xxiv] The purpose of the workshop (and the subsequent invitation for public comment) was to obtain public and expert input on the privacy and security concerns raised by the IoT. The Commission then published a report in January of 2015, summarizing the workshop and providing staff recommendations on key issues, including commentary on how long-standing Fair Information Best Practices (FIPPs) may help to protect consumer privacy.[xxv] The following suggested measures, taken in

As technology rapidly advances, there are a number of preventive measures and best practices that device manufacturers and developers (and their legal counsel) can put into place to alleviate some of the potential privacy, liability and data accessibility concerns.

part from the FTC's 2015 report, are just a few potential considerations for managing wearable device data; manufacturers and software developers should fully review applicable federal and state laws and regulations in the context of their specific device(s).

Have a Plan

Having a plan in place may seem like an obvious first step. However, this can be surprisingly challenging when it comes to rapidly changing technologies. Knowing the answers to questions such as the following can go a long way in allowing a company to understand and manage the risks associated with wearable technology:

- Will the wearable device involve the collection or transmission of data that meets the definition of "protected health information" (PHI)?
- Will the device potentially treat a specific illness, injury or condition, thereby triggering the possibility of FDA regulation as a "medical device"?
- What parties are involved in the supply chain, from manufacturing to actually delivering the product or services to the end user?
- Where and how will data be stored?
- What parties will have access to the data being collected or transmitted?

Safeguard the Data

Adopting reasonable security measures will inevitably depend on a variety of factors, including the volume and sensitivity of collected data, as well as the costs associated with correcting any future security breaches. Thus, different approaches to security may vary quite a bit. However, there are a number of best practices that may be worth consideration in order to secure potentially private data.

First of all, consider building security into wearable devices at the outset. This may include conducting a risk assessment and testing device security before it is released into the market. Providing training to all employees on proper security practices may also help to proactively address potential security issues.

In a 2013 study, researchers investigated mobile health and fitness application data practices and identified several key privacy risks involved with mHealth app usage.[xxvi] According to the research, the biggest privacy risks were primarily due to unencrypted connections to third-party advertisers and analytics services. For example, one unnamed "well-known" company's app allowed users to research information about specific drugs. The names of drugs researched by users were then sent to a third-party advertiser, who was able to then link that data to the specific user's web browsing history. Based on this research, it is strongly advised that mHealth data not be transmitted to third-party advertisers and analytics service providers.

Wearable device and mHealth app manufactures and developers may also wish to consider other potential information security practices, such as:

- Providing – and adhering to – a carefully crafted privacy policy;
- Enabling device or app-level passwords or multi-factor authentication;
- Implementing auto-wipe features to minimize the risks associated with lost or stolen devices;
- Using encrypted network connections for data transmitted between the app/device and any internet server; and
- Performing ongoing security evaluations and penetration testing.

Data Minimization

Similar to HIPAA minimum use and disclosure rules, which require covered entities to take reasonable steps to limit each use or disclosure of PHI to the minimum use or disclosure necessary to accomplish a relevant task, the concept of "data minimization" encourages companies to limit the consumer data they collect and retain, as well as dispose of any data that is no longer required for device functionality. Implementing reasonable limits on the collection (and retention) of consumer data may help to alleviate two security-related risks:

1. **"Treasure troves,"** or large volumes of collected and stored data, may attract would-be data thieves, thereby increasing the risk of a data breach.

2. **Collecting information** that is not strictly necessary to the device's intended functionality may result in usage that deviates from the end-user's reasonable expectations (such as selling data to third parties for advertising or other purposes), thereby triggering potential consumer privacy concerns and investigations.[xxvii]

Device manufacturers and developers should consider the following:

- Do not collect or store data that is not necessary for intended use or functionality of the device.

- Limit individual and third party access to collected data.

- Consider whether all aspects of the device, software or data require connection to, or transmission through, the internet. In many cases, the device itself may be able to store and/or process certain data without the use of an internet connection, which can help limit potential access to the data.

Notice and Choice

Depending upon the type of data being collected or used, wearable device manufacturers and developers may benefit from building "notice and choice" functionality into the device, or portions of the data being collected. This typically entails some form of notice to the consumer that certain fields or types of data are being collected, often pairing this notice with the ability to "opt out" of certain data collection or usage practices. This is typically accomplished by automatic alerts when the device is first being set up or used, or when specific fields of data are being collected (consider iPhone alerts when an app is about to use or track GPS location services, or access a user's contact list).

To be certain, notice and choice capabilities often pose practical difficulties for use in wearable devices, which may or may not have user interfaces that are set up to display notice and choice alerts. Device manufacturers and developers will need to balance the need for this type of security measure with the overall purpose and design of the device. In its 2012 *Privacy Report*, the FTC stated that companies need not provide choice before collecting and using consumer data for purposes consistent with the consumers' reasonable expectations. [xxviii] This concept was reiterated in the Commission's *IoT report* and could be reasonably applied to wearable devices.

IV. On the Horizon

Rapid advancements in medical technology will almost inevitably result in significant changes to the litigation landscape. In fact, we are only seeing the proverbial "tip of the iceberg" when it comes to mHealth and wearable technology capabilities. Smartphone sensors that can monitor exposure to radiation, air pollution and even pesticides are currently in development.[xxix] Within the next two years, it is predicted that Americans will be able to wear wristwatches that continuously monitor blood pressure and other vital signs, as well as the level of fluid in the lungs. Contact lenses will be able to track glucose levels or eye pressure, and head bands will have the ability to track brain wave activity. Nanosensors embedded within the bloodstream could survey for cancer, autoimmune attacks, or cracks in artery walls that could lead to heart attack or stroke.

And back to the aforementioned "smart tattoo"? The company behind Fitbit®, NewDealDesign, has answered a conceptual design challenge with what it sees as the next step in wearable technology: Project Underskin.[xxx] Project Underskin is a "smart digital tattoo," which would be implanted into the wearer's hand. The tattoo would allow for capabilities such as unlocking doors using near field communication (NFC) technology, tracking the body's health, or exchanging information through a handshake – all done through touch. According to NewDealDesign, the current state and pace of electronics research could allow for this tattoo to become a reality in as little as five years.

What's Next?

Is the data generated from wearables and other mobile apps interacting with patient medical records? LMI's next MIM publication will discuss electronic health records (EHRs), with a focus on the intersection of medical records and "big data."

For now, smartphone "selfies" are at the height of popularity, but smartphone physical exams are only just being introduced. Apple's iPhone now boasts CellScope, which is an otoscope that allows parents to capture a video of a child's eardrum and share the results with their pediatrician.[xxxi] The ability to make a definitive DIY diagnosis of an ear infection with a phone is just the first step. Apps are now being developed to handle all aspects of the eye, the throat and oral cavity, and the lungs and heart.[xxxii] Meanwhile, nearly all sophisticated medical imaging devices are being miniaturized: hand-held ultrasound devices are already available, and some medical schools have begun issuing them in the place of old-school stethoscopes.[xxxiii] Hand-held magnetic resonance imaging (MRI) machines aren't far behind, and engineers at UCLA have come up with a smartphone-sized device that can generate X-rays. "It won't be long before you can take a smartphone X-ray selfie if you're worried that you might have broken a bone." [xxxiv]

Just as the dot-com boom forced the courts to grapple with existential questions such as Internet jurisdiction and communications that make geography an after-thought, the IoT evolution, including wearable medical devices, will take its turn to gradually shape future case law – for product liability, medical malpractice, information security, and many other areas of law. There is a great potential for data vulnerability if the devices, and their transmission of information, are not carefully secured. Strap on those wearable devices (and your seatbelts), as the future of medical technology is bound to be quite a ride.

THANK YOU for subscribing to the MIM Reporter!

If you would prefer to receive your copy of the MIM Reporter electronically, please send us an email containing your name, firm name and email address to: **research@lmiweb.com**

Litigation Management, Inc.
6000 Parkland Boulevard, Mayfield Heights, Ohio 44124 | 800-778-5424 (ph) 440-484-2020 (fax)
Published as an educational service to the Corporate, Insurance and Defense Legal Community.

references

[i] "James Geddes, "Fitness Trackers Up To 40% Inaccurate; Fitbit, Jawbone, Nike, Others Tested in New Study, Which Performed Best?" Tech Times, January 18, 2015, http://www.techtimes.com/articles/27248/20150118/fitness-trackers-up-to-40-inaccurate-fitbit-jawbone-nike-others-tested-in-new-study-which-performed-best.htm.

[ii] Jonathan Cain, "Wearable Devices in the Workplace Challenge Data Security and Privacy," Mintz Levin Privacy & Security and employment, Labor & Benefits Advisory, August 21, 2014, http://www.mintz.com/newsletter/2014/Advisories/4200-0814-NAT-PRIV-ELB/4200-0814-NAT-PRIV-ELB.pdf.

[iii] Mike Feibus, "2015: The Year of Health Care for Wearables," Special for USA TODAY, January 5, 2015, http://www.usatoday.com/story/tech/columnist/2015/01/02/wearables-fitness-is-name-of-the-game-but-healthcare-is-where-its-at/21190395/.

[iv] "Are You Willing to Share Your Wearables Data with Your Boss?" NPR Morning Edition, June 2, 2015, transcript available at http://www.npr.org/2015/06/02/411406418/are-you-willing-to-share-your-wearables-technology-data-with-your-boss.

[v] See U.S. Department of Health and Human Services, Food and Drug Administration, "General Wellness: Policy for Low Risk Devices, Draft Guidance for Industry and Food and Drug Administration Staff," Center for Devices and Radiological Health, February 9, 2015. See also U.S. Department of Health and Human Services, Food and Drug Administration, "Mobile Medical Applications, Guidance for Industry and Food and Drug Administration Staff," Center for Devices and Radiological Health, February 9, 2015. See also U.S. Department of Health and Human Services, Food and Drug Administration, "Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices, Guidance for Industry and Food and Drug Administration Staff," Center for Devices and Radiological Health, February 9, 2015.

[vi] U.S. Department of Health and Human Services, Food and Drug Administration, "General Wellness: Policy for Low Risk Devices…", supra.

[vii] Colin Lecher, "The FDA Doesn't Want to Regulate Wearables, and Device Makers Want to Keep It That Way," The Verge, June 24, 2015, http://www.theverge.com/2015/6/24/8836049/fda-regulation-health-trackers-wearables-fitbit.

[viii] Adam Satariano, "FDA 'Taking a Very Light Touch' on Regulating the Apple Watch," Bloomberg Business, March 30, 2015, http://www.bloomberg.com/news/articles/2015-03-30/fda-taking-a-very-light-touch-on-regulating-the-apple-watch.

[ix] Brian Dolan, "FDA Clarifies the Line Between Wellness and Regulated Medical Devices," MobiHealthNews, January 16, 2015, http://mobihealthnews.com/39775/fda-clarifies-the-line-between-wellness-and-regulated-medical-devices/. See also the FDA's "Decision Algorithm," as set forth in the U.S. Department of Health and Human Services, Food and Drug Administration, "General Wellness: Policy for Low Risk Devices…", supra.

[x] U.S. Department of Health and Human Services, Food and Drug Administration, "Medical Device Accessories: Defining Accessories and Classification Pathways for New Accessory Types, Draft Guidance for Industry and Food and Drug Administration Staff," Center for Devices and Radiological Health, January 20, 2015.

[xi] Id.

[xii] Adam Satariano, "FDA 'Taking a Very Light Touch…", supra. See also Varun Saxena, "Federal Trade Commission Cracking Down on Questionable Mobile Medical Apps," Fierce Medical Devices, March 27, 2015, http://www.fiercemedicaldevices.com/story/federal-trade-commission-cracking-down-questionable-mobile-medical-apps/2015-03-27.

[xiii] U.S. Federal Communications Commission, "FCC Chairman Announces New Connect2Health Task Force," Commission Document, March 4, 2014, https://www.fcc.gov/document/fcc-chairman-announces-new-connect2health-task-force.

[xiv] Debra Dunne, Wendy Williams and Virginia Knapp Dorell, "Analyzing Risk in Mobile Medical Apps," Update Food and Drug Law, Regulation and Education, a publication of the Food and Drug Law Institute, November/December 2014.

[xv] Michael H. Cohen, "What 2015 Will Bring for Wearable Tech," Daily Journal, December 16, 2014, http://michaelhcohen.com/circlestest/wp-content/uploads/2014/12/Wearable-Health-Tech-12-16-14-Cohen-PDF.pdf.

[xvi] Id.

[xvii] Sue Ter Maat, "Health, Fitness Apps Pose HIPAA Risks for Doctors," American Medical News, August 5, 2013, http://www.amednews.com/article/20130805/business/130809993/7/.

[xviii] James Geddes, "Fitness Trackers Up To 40% Inaccurate…", supra.

[xix] "Wireless Blood Pressure Monitors and Blood Glucose Meters Don't Measure Up," ConsumerReports.org, March 3, 2015, http://www.consumerreports.org/cro/news/2015/03/wireless-blood-pressure-monitors-and-blood-glucose-meters-don-t-measure-up/index.htm.

[xx] Pam Baker, "Mobile Health Apps, Part 4: Life, Death and Lawsuits," TechNewsWorld, ECT News Network, May 5, 2011, http://www.technewsworld.com/story/72394.html.

[xxi] Id.

[xxii] Kate Crawford, "When Fitbit Is the Expert Witness," The Atlantic, November 19, 2014, http://www.theatlantic.com/technology/archive/2014/11/when-fitbit-is-the-expert-witness/382936/.

[xxiii] Id.

[xxiv] U.S. Federal Trade Commission, "Internet of Things – Privacy and Security in a Connected World," FTC Staff Report, January, 2015, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[xxv] Id.

[xxvi] Linda Ackerman, "Mobile Health and Fitness Applications and Information Privacy – Report to California Consumer Protection Foundation," Privacy Rights Clearinghouse, July 15, 2013, https://www.privacyrights.org/mobile-medical-apps-privacy-consumer-report.pdf.

[xxvii] Craig Michael Lie Njie, "Technical Analysis of the Data Practices and Privacy Risks of 43 Popular Mobile Health and Fitness Applications," Privacy Rights Clearinghouse, July 15, 2013, August 12, 2013, https://www.privacyrights.org/mobile-medical-apps-privacy-technologist-research-report.pdf.

[xxviii] U.S. Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," Commission and Staff Reports, March 2012, https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

[xxix] Eric J. Topol, "The Future of Medicine Is in Your Smartphone," The Wall Street Journal, The Saturday Essay, January 9, 2015, http://www.wsj.com/articles/the-future-of-medicine-is-in-your-smartphone-1420828632.

[xxx] "From the Designers of Fitbit, A Digital Tattoo Implanted Under Your Skin," Fast Company, Inc., Wearables Week, October 1, 2014, http://www.fastcodesign.com/3036175/from-the-designers-of-fitbit-a-digital-tattoo-implanted-under-your-skin.

[xxxi] Lisa Fratt, "Say What? An iPhone Tool to Diagnose Ear Infection?" Thriving, Boston Children's Hospital Pediatric Blog, posted January 28, 2015, http://thriving.childrenshospital.org/say-iphone-diagnose-ear-infection/.

[xxxii] Eric J. Topol, "The Future of Medicine Is in Your Smartphone," supra.

[xxxiii] Rebecca Greenberg, "Making Waves: Ultrasound Use Increases in Medical Education," Association of American Medical Colleges AAMC Reporter, December, 2012, https://www.aamc.org/newsroom/reporter/dec2012/323592/ultrasound.html.

[xxxiv] Eric J. Topol, "The Future of Medicine Is in Your Smartphone," supra.