Doctor, Doctor, Give Me the News

New iPhone and Other “Health” Apps May Have Security and Regulatory Issues

By Mark Rasch

At a recent CISO conference in New York, the conference sponsor gave all of the attendees (yes, all of the attendees) a Fitbit device that measures their physical activity. [Disclaimer here: the sponsor was SecurityCurrent – pretty cool.] The device is worn on the wrist and measures the exertion and exercise of the wearer, shares that data with a computer or a web app, and also can share that data with other Fitbit users or onto social networking sites like Facebook – all at the option of the user. Alternatively, you could go to the local Home Depot and attach the device to the paint shaker and really impress your friends.

So continues the first baby steps into the “Internet of Things” in the health-care arena. Apple will be releasing the new iPhone 6 (another conference giveaway, please?) which, according to reports, will include a host of apps and integrated functionality to promote the health of users.

Apple is betting on the mobile health strategy. Its new HealthKit, embedded in iOS 8 is http://appleinsider.com/articles/14/06/03/ios-8-first-look-video-apples-health-app-and-emergency-medical-id designed to integrate with a host of healthcare monitoring applications or peripherals and immediately alert both the patient (um, user?) and their healthcare provider when their medical conditions meet or exceed certain parameters. When that happens, the local first responders could be called, with the iPhone acting as both medical record, medical alert bracelet, and tattletale (my iPhone subscriber has fallen and I can’t get up!) Great if your insulin levels show hypoglycemia, or ketoacidosis or hypertension. Slap one onto a substance abuser and call both the ambulance and the probation office. Blood alcohol level exceeds .08 while MPH exceeds 15? (jogging drunk is ok). Not only evidence for DUI conviction, but the phone’s location and subscriber’s name is sent to the State police. Sure, public safety -- but at what price? Such tools could be useful for dealing with the upcoming Zombia apocalypse, but do you really want Brad Pitt cutting your hand off because your iPhone says to? Well, maybe --it is after all Brad Pitt, right?

No don’t get me wrong. Increasing exercise, improving diet, reducing smoking, and reducing obesity are all good ideas which may – or may not – in the long run save society money. (live longer, receive Social Security longer, right?) So we have current (and near term future) devices like the Nike in shoe sensor http://www.nike.com/us/en_us/c/running/nikeplus/gps-app or Wahoo Fitness devices, and Withings all of which measure your running from the gym to the bakery, and which can then report your progress to your doctor, weight watcher’s support group, or the local Alocolics Anonymous meeting. Chips embedded in phones can measure blood pressure and cholesterol http://www.ibtimes.com/apple-iphone-6s-new-chip-will-measure-blood-pressure-cholesterol-more-1668370 and track this data over time. But as we adopt Internet, networking and social networking technologies to health care and health related products and
services, we must be mindful of the ways that the data generated from these devices may be used – and abused, not just today but generations from now.

A few examples.

- Some 30 years ago, a Miami cop friend of mine was involved in the search for a serial rapist. DNA technology was just coming into the fore, to the Miami-Dade PD decided to enlist male members of the public who met the general description of the rapist (bipedal hominoid, male) to “voluntarily” provide DNA samples – a cheek swab – to be compared to the results from the rape kit. I use the quotes around “voluntary” because the names of people who refused to consent were provided to the Miami Herald for public shaming. (“got something to hide Mr. Camacho?”) In this way, Metro Dade collected DNA samples from more than 30,000 people – none of whom matched the suspected rapist. So what did the police do with the samples? They kept them and are using them to this day for “familial” DNA matching. So some 20 year old who gave a DNA sample in 1985 has a nephew born in 1995. That nephew may be (properly or improperly) implicated in a crime by virtue of his mom’s brother’s DNA sample 30 years earlier. Scope, purpose and duration, folks.

- In another case, the so-called BTK murders (Bind, Torture, Kill) a serial murderer abducted, raped and tortured women in the Midwest for decades. Although he stopped for more than 20 years, when he restarted in the late 80’s he mailed a floppy disk to the local newspaper containing a file. The disk contained evidence that lead the police to a volunteer at a local church – a suspect in the multiple murders. They had crime scene DNA, but not the suspect’s DNA. So they went to the suspect’s sister’s gynecologist and obtained her most recent PAP smear (under federal law PAP smears must be kept for several years to compare for abnormalities). Using the same familial DNA, they linked the church volunteer to the multiple murders. Good result, right?

- Similarly, the CIA used the cloak of an immunization program in Abadobad, Afghanistan to help look for DNA associated with Usama Bin Laden. Though the results were somewhat useful, as a result of the “ruse” not only are thousands of children no longer getting immunized (and dying as a result), but hundreds of health workers are being murdered by the Taliban and associated organizations.

- By examining certain sales patterns (e.g., decrease in alcohol purchases, increase in Folic Acid sales) Target was able to predict which of its customers was pregnant, and tailor both mailings and email marketing campaigns to them. In one case, a father of a teenage girl first learned of his daughter’s pregnancy when the Minneapolis retailer sent mailings for strollers, onesies and diapers. Happy grand-father’s day from Target.

- I was involved in a security assessment of an RFID-enabled implantable pacemaker. Rather than requiring physical leads, the telemetry from the pacemaker could be scanned to an app, and the software updated remotely. Pretty cool. And approved by the FDA. With absolutely no authentication or security. Ooops. (Problem fixed though.)
You see medical information – and related health information – is far too sensitive to be treated the way we treat it today. Integrating healthcare functionality into smartphones, fitbits, breathalizros, home screening tests and the like may be a great idea, but doing so without considering the privacy and security aspects thereof is just plain stupid. If your Android device measures and tracks your blood pressure, is it now a medical device subject to FDA regulation or approval? What if the information it collects is used for diagnosis and treatment? Can a life insurance company base its rates on your fitbit results, and if so, can it subpoena those from your phone?

I haven’t “seen” a doctor in years. Whenever I need a doctor, I dial up (ok, I haven’t seen a dial in years either) my identical twin brother and ask him for a diagnosis. If it’s a twisted ankle or a sprain/strain, I take a quick iPhone shot (or Facetime) and he tells me to take two aspirin and call him in the morning. If the diagnosis requires lab tests or radiology, I simply have HIM give blood or get x-rays (the advantage of identical twins, no? Spare parts.) While this may represent an extreme example, many new services offer physician or nursing advice through apps and smartphones. But these raise their own concerns about privacy, security, authentication, HIPAA compliance, and even licensing and payment (was this an “office” visit? Where was the “office” located?)

So just a few issues for the next generation (version 1.5) of mobile health devices.

1) Privacy
What data is being collected. Why? For what purpose? In what way? How is it being used? Is there a privacy policy associated with the app or device? How are these communicated? Opt in? Opt out? EU and other data privacy regulations for sensitive personal information? Sometimes, merely wearing the device reveals a diagnosis or treatment of a patient. If the device is too overt, it may itself constitute a HIPAA violation, or at least an issue.

2) Security
How is the information protected throughout its life-cycle? What does the device measure, and how? Can the device be corrupted if lost or stolen? How does the device communicate? What is stored on the device and how?

3) Authentication
If the device communicates with others or online, how are the devices, the people, and the network connections authenticated? Remember though, strong authentication of identity means strong attribution, and therefore less privacy.

4) Data collection
What data does the device collect (and metadata too) and for what purposes? I think the fitbit on my wrist uses an accelerometer to collect data about movement, from which it infers calories burned. But it also collects data about WHEN (and possibly where) the activity occurred. So it could know when I go to sleep (and with whom if the other person is a fitbit user and our
patterns match – 11:30 to 12:15, PM, heavy exercise followed by rest?) It can know when I actually woke up. Teleworkers could have their activities monitored by employers (billed us for a cat nap, eh?) By linking the fitbit to the cell phone which has GPS, the device can map the user’s activity. Just as the CIA uses “gait” analysis as a biometric to identify specific individual, accelerometer patterns may become so unique as to ID people as well. Thus, the nature and volume of data collected may at first seem innocuous – it’s just accelerometer data. Until it isn’t. (It’s all fun and games until someone loses an eye – or privacy.)

5) Data use
Related to data collection is data use. Sure, I can use the fitbit data to get my lazy butt off the couch (just two more innings, mom!) But if the data is collected and transmitted to others, or collected by the app developer, device manufacturer, internet or other connection provider, or some service provider, how are THEY using the data? Here, a simple privacy policy doesn’t do the trick. Nobody wants to read hundreds of privacy policies for their phone, their internet connection, their shoes, their T-shirt, and their underwear (I think my boxers are spying on me.) What’s worse, these policies are written by the very companies that may make money on your data and have a vested interest in continuing to do so. And everyone has a different tolerance for privacy – or perceived tolerance. If you told those Miami volunteers the (unintended) consequences of their volunteer acts, would they have made the same decisions in the 1980’s? I suspect not.

6) Data aggregation
Almost as bad as data use is data aggregation. Your personal data may get thrown into a pile with that of others for trends, public health or other reasons. This may enure to your benefit (surprise! You get lower insurance rates) or to your disadvantage. Ooops, our software predicts that you are a zombie. Related to aggregation is data mining – looking for patterns in these masses of aggregated data. I recently read a statistic that redheads need more anesthesia to put them under. Interesting and possibly useful. But WHO decided to look at anesthesia amounts by hair color? Now your anesthesiologist can charge you more because you are a ginger. Oh, and blondes have more fun, right? Check the fitbit between 11:30 and 12:15 to see if that is statistically correct.

7) Data transfer
Many “smart” health apps rely on the transfer of data from the device to something else – a nearby Bluetooth device, a smartphone, the Internet, other users. As we see in the PCI arena, even encryption schemes don’t secure data which may be transferred in the future (the instant between magstripe reading and data encryption). So vendors must examine the data lifecycle through its entire process. Moreover, data networks designed for email and text may not be appropriately secure when used for sensitive health information. Remember, the Internet was designed for resiliency, not security.

8) Data availability
What good is health information if it can’t be used? What happens if the device breaks? I have a bunch of old emails and files stored on my ZIP and JAZ drives. Good luck getting to it. And don’t even ask about the 8” floppies. Because many of these health and health care devices rely on interconnected devices (measuring device, smartphone, app, Bluetooth connectivity, WiFi connectivity, website operation, cloud storage) a failure of any of these (or a breakdown in security of any of them) may result in a failure of the data itself. That’s fine if all you are measuring is the number of chin-ups you can do at 6AM (um.. three, but AFTER coffee) but not so great if you are measuring inverted T waves on an EKG through a droid. (We’re going to have to reboot grandpa.)

9) Data longevity
Persistence. It’s great for marathoners. Not great for data. Data is collected for a purpose. If data outlives that purpose, it has the potential for abuse. Moreover, we rarely expend energy to protect “old” data. Remember that JAZ drive? It’s sitting in a cardboard box in my garage, next to the Gordian knot of data, power and sync cables. Medical data persistence may prove very useful, or extraordinarily misleading. Data indicating that patients whose parents took Thalidomide in the 1960’s may suffer particular disorders in the 21st century can be useful for epidemiologists and product liability lawyers alike. But persistent data may also increase the number and severity of false correlations as well. As a result, we may not give mammograms to women under 60 (save money, right?) or we may not pay for it. This is all part of “evidence based medicine” which is great if based on real evidence with real validity. If not, not so great.

10) Data and device reliability
As we rely on these “medical” devices, we must know that both the device itself and the data collected and generated by the device are accurate. Wait, my blood pressure is 500 over 12? Are you SURE? In the horror (I meant horrible) movie, The Net, comedian Dennis Miller is killed when hackers change the data from medical devices leading to the wrong diagnosis and treatment. (the patient, and Miller’s career, could not be revived.) In Homeland, the Vice President’s pacemaker is remotely hacked (hear THAT Mr. Cheney? ) All potentially possible but implausible. It’s hard to hack a leech, though.

11) Product Liability
This one is huge. When we transform a consumer device like a phone or a tablet into a mission critical life-saving patient dependent medical device, we expect that it will operate continuously and properly. Ok, you can get off the floor from laughing now. We don’t expect to have to reboot our sphygmomanometer, or wait for 3 bars for our EKG to work. Moreover, as multi-use devices, mobile devices are subject to a wide variety of attacks for a wide variety of motives with a wide variety of impacts. Someone trying to steal our bank PIN number (doesn’t the N in PIN stand for Number?) my inadvertently (or deliberately) shut off or alter medical information. (“Bad news -- your aunt is dead AND she has no money in her account!”) This liability will run to the device, the peripherals, the hardware, the chips, the sensors, the software, the network and
the aggregators and collectors as well. The answer will either be safer more secure devices (ha!) or click-wrap “terms of use” where mobile device users absolve the product of any liability. Just like when your GPS tells you to drive into a ditch.

12) Data Portability
What happens when the fitbit is replaced by a competitor’s bitfit? Can I move the important health data? HIPAA allows patients to have access to their medical records. Are the results of these devices, medical records? Does it matter who collects them? Where the data is collected? If the data remains locked to a device, and the device locked to a provider, then the data is not useful or portable. (“It would be a shame should anything happen to dis here nice blood pressure data. Fuggetaboutit.”)

13) Ownership
Whose life is it, anyway? Who “owns” – as in has the right to use, transfer, etc., the data collected by a remotely accessible device? Who has the right to consent to a search or seizure of, or use of that data? How do we apply the “third party” data rule to this information? Is the fitbit website that f a medical “provider?” Stay tuned for next week’s episode to find out.

14) Secondary use
Once the information is collected, how ELSE will it be used. Typical explanations of uses of personal information are either incomprehensible, ambiguous or just wrong. A human should know how their data is being used and to have some meaningful control over its use.

15) Data processing and third party access
Once having been collected, the data is likely to then be “processed” by some data processor. This at a minimum means that it will be held by third parties (fourth, fifth and sixth parties) with their own data use and data privacy policies in countries anywhere in the world. Data about your alcohol use may be residing in servers at the Guinness brewery in Dublin. Which might not be an altogether bad thing. Are we having fun yet?

16) Inadvertent or Negligent Use
Related to security is the problem of inadvertent or miscellaneous use. Simple example. A user with sensitive information also decides to download kiddie porn. Police are called and the man escorted in handcuffs. The entire hard drive – with your sensitive medical information – is now in the hands of the Sheboygan, Wisconsin police department. The more data we collect, the more data will leak. And in diapers and data, leakage is bad.

17) Device transfer
I sell my fitbit to another person. What happens to the data that was on it? Who wipes it and how? It’s hard enough when we transfer, sell, or lose a device we KNOW has data on it (thumb
drive, phone, computer). Now we may need to wipe our sneakers, t-shirt or hat -- well, at least the data therein.

18) FDA approval

So what’s the role of the US FDA in all this? Medical devices -- whatever those may be - - have to be approved by the agency. The FDA has issued regulations and guidance on how it will regulate mobile devices and apps. It [http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ConnectedHealth/MobileMedicalApplications/ucm255978.htm](http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ConnectedHealth/MobileMedicalApplications/ucm255978.htm) has adopted a “risk based approach” to the regulation of mobile medical devices, lightly regulating “low risk” devices (maybe the fitbit or pedometer apps), and taking a different approach to moderate risk (Class II) or high-risk (Class II) mobile medical devices. The guidance also provides examples of mobile apps that are not medical devices, mobile apps that the FDA intends to exercise enforcement discretion and mobile medical apps that the FDA will regulate. So not all apps are created equal.

19) Connectivity and FDA approval (end to end?)

So, when is a device a device? Something like the AliveCor Heart Monitor [http://www.fastcodesign.com/1671371/this-200-iphone-case-is-an-fda-approved-ekg-machine](http://www.fastcodesign.com/1671371/this-200-iphone-case-is-an-fda-approved-ekg-machine) is an iPhone case that can be held in the user (patient’s) hands (or clutched dramatically to the chest if you are Red Foxx) is an FDA-approved iPhone case that can be held in your hands (or dramatically pressed against your chest) and generates an EKG. The device itself presents at least moderate risk that it won’t work or won’t be accurate, so it is subject to (and has received) FDA approval. Fine. But what about the app that collects the information FROM the AliveCor? Or the one that stores it? Or the one that transmits the data to the doctor or pharmacy? Are these subject to FDA approval too? It’s not enough to sense data and collect it. We need data integrity and availability throughout the data lifecycle -- which may mean FDA approval of everything.

20) Telemedicine

Another issue related to the use of mobile devices for healthcare relates to telemedicine. When you phyically separate the “patient” from the provider, you run into a host of legal issues. For example, does the physician get paid for an “office”visit when he or she reviews the telemetry data from the patient? What constitutes an office visit for the purposes of reimbursement? Which state/country’s standard of care, liability law, or other laws apply to a remote provider and a local patient? Are disclaimers contained in a web app -- not just on privacy but on liability and other issues -- sufficient to constitute both notice and consent in the healthcare arena -- particularly when we know that nobody ever reads them? What constitutes the “practice of medicine” when non-medical personnel (e.g., software engineers, etc.) are writing code designed
to flag medical conditions? OK. My head hurts now. Perhaps 2 aspirin?

21) Licensing

Related to the telemedicine problem is that of licensing. Every state wants to control those who “practice” in their jurisdiction. But what constitutes the “practice” of medicine? So if a doctor in Bangladesh is giving advice based on monitoring of a web app in Brooklyn, does the doctor have to be licensed in New York? Magic 8 ball says -- “situation hazy -- ask again later.”

22) Data “breach” definition for devices

All kinds of laws, including HIPAA and HITECH require notification when there is a “breach” -- that is, the unauthorized access to or use of Personal Health Information (PHI). Cool. So if I lose my phone with the shared data from 1,000 friend’s fitbits, is that a “breach?” Does the data have to be private, semi-private or otherwise protected to be subject to the breach laws? As date becomes more portable, it becomes more at risk. Encryption might be nice, but these mobile devices rarely use or support it. Mo’ data = mo’ problems.

23) Remote wipe?

Do we want to give someone the ability to remotely wipe PHI from a device? What if this is the only copy of that data? What if the data is the evidence of medical malpractice or device malfunction? I love it when a plan comes together.

24) Public health

Should public health officials have the ability/authority to override privacy controls when there is a Zombie apocalypse? Can they access people’s cell phones to search for the undead? What about monitoring devices connected to these devices -- or the data itself. Remember, it takes 13 seconds to turn into a zombie -- so if you haven’t changed by then, you probably won’t.

25) Data aggregation anonymity issues (de-identified)

Data anonymity relies on the fact that we don’t disclose the patient’s name. Ubiquitous health monitoring together with big medical databases essentially eliminate those protections. “Patient is a 28 year old female in Los Angeles, California (DOB 7/2/86) treated for repeated substance and alcohol abuse. Ht., 5’5”, weight 110 lbs, four siblings, etc.) Oh, thank you Miss Lohan. Did I mention ‘mo data = ‘mo problems?
So all of these things need to be considered when creating a worldwide accessible mobile and unsecure healthcare database. What could go wrong? At least you can’t hack leeches. Or can you?