Sonia E. Arista

Advisor - Linn Freedman

EMCS 2019 Executive Program Resources - Critical Challenge Project

29 December 2018

Security Considerations for Mobile Health Application Use

Challenge Overview

My challenge outlines the lack of governance and review observed in the healthcare provider environment with the use of "market " or "consumer" clinical and medical mobile applications as resources for informing or influencing a course of care. My position is that as more mobile applications are readily adopted and pervasive within clinical practice they should be vetted like any other enterprise "sanctioned" resource. In a controlled provider environment, these applications should go through the same review process (security, integrity, functionality) as any other IT sanctioned software used in the clinical setting; in the patient safety context, I aspire to raise awareness against submission of protected health data and other personal data to application sources for which the validity and integrity of the solution is unknown. In conclusion, I will outline current and proposed methods for raising general awareness and governance for mobile health applications and hypothesize on the collective societal benefit of a more rigorous review process.

In order to provide context to the reason that I chose this particular subject matter for my Critical Challenge Project focus, I will share with you a personal experience. Five years ago, my youngest child was two weeks into starting Kindergarten when we discovered a small lump on the back of her leg. A few days after she started to complain of joint aches, and with trips to

local pediatricians, we were referred to a large and prominent academic medical center to conduct radiological scans. My daughter was quickly diagnosed with a rare and aggressive pediatric muscular cancer. At the time of discovery, the cancer had already metastasized quickly and she was in a "Stage 4" classification of progress. Diagnosis and treatment, including chemotherapy and radiology, began almost immediately. For the next year, our family was quickly initiated into a world of cancer terminology, inpatient experiences, and medical technologies that were previously unknown.

At the time, I had already held the position of a Chief Information Security Officer at another local academic medical center for a few years. I was familiar with the hospital setting and applications that support clinical workflow, but to that point only from a distance through various IT implementations and clinical service enhancements. As the CISO, I was not only aware of the rapid proliferation of mobile devices in the environment, but also had some personal experiences with mobile device use leading to privacy and security incidents at the hospital.

After a few weeks of treatment, my daughter's care team informed me of the details behind her rapid diagnosis and identification of the oncology specialist. As she was getting her initial radiology scans, one of the technicians in the room took a picture on their personal mobile phone and sent the image to an oncologist who was at a conference in Europe. This oncologist, upon seeing the image (and I assume corroborating the diagnosis within the other details within the electronic medical record) immediately took my daughter on as a patient and outlined initial treatment steps.

Although the details of what applications or transfer of data method the technician used are unclear, upon hearing this story, as a security professional my initial thoughts were - Was it an approved application? Was it sent through a personal text message? Is the image, in fact, still

on the phone or perhaps in a cloud repository to this day? What if the image was of low quality or some component was obscured or unclear? Would that have affected the course of treatment or diagnosis?

Over the next several months, I made other observations of nurses and clinicians referencing or using their mobile devices over the course of my daughter's treatment and care - this was consistent with what I had increasingly seen in my own institution. Thankfully, we had a great outcome and she has been in remission for 5 years with no complications. At the time, as the mother of a patient, I was in an incredibly vulnerable state of relying on the professionalism of her caregivers, and trusting their choices for her care. As a panicked and stressed mother, I felt grateful that the information was able to reach the right people at the right time, however I could not help but wonder to what effect this mobile technology had a direct impact on our experience. Only in hindsight, am I able to reflect and explore the implications from a data security perspective and hypothesize on how these methods may affect patient care, the implication of the use of these tools in the care setting, and the considerations that need to be made in regards to data security, integrity and availability.

"Sanctioned" vs. "Unsanctioned" Medical Applications

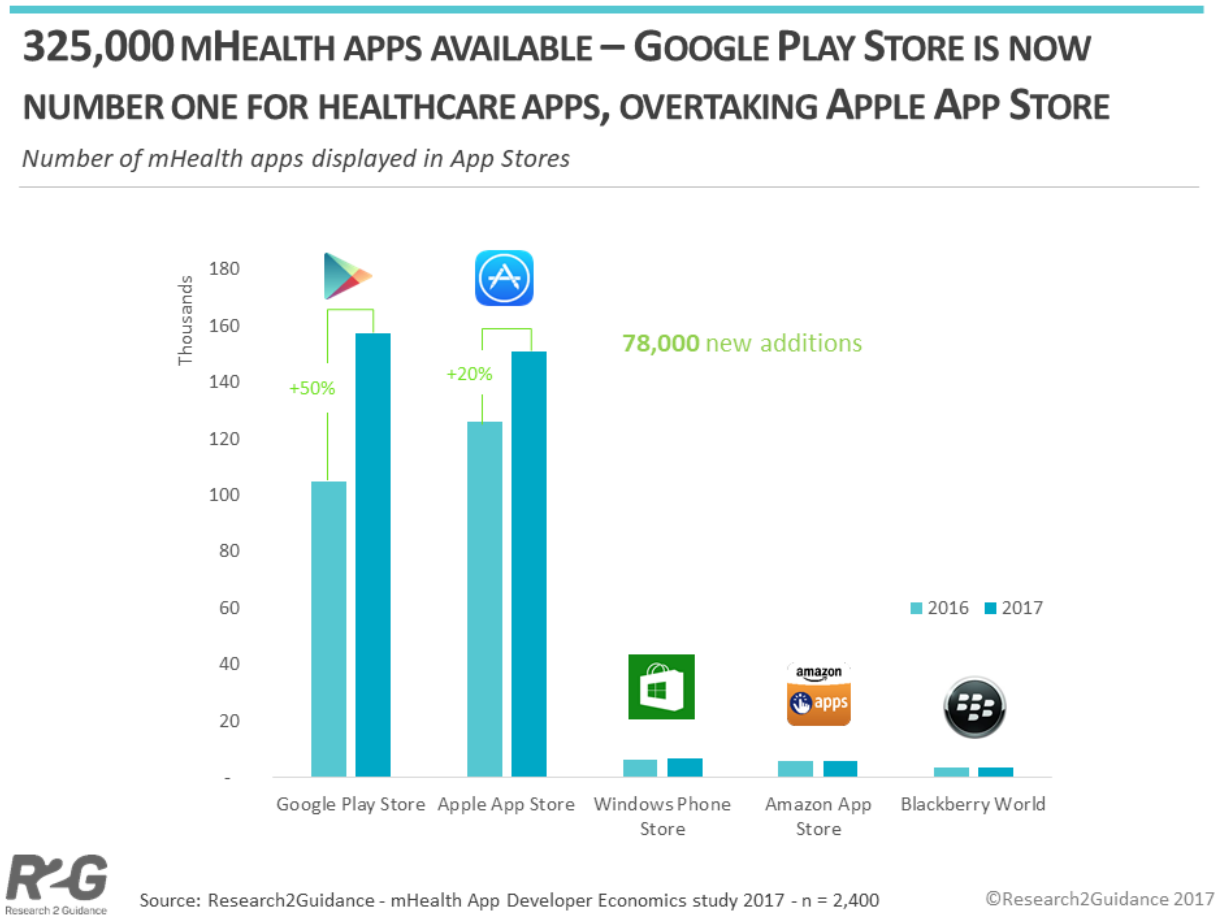
In any business or organization that uses technology enablement, the information services operational area typically has resources dedicated to "applications support." This function exists to support the software application portfolio of all of the applications that have been purchased or licensed to the enterprise. In the case of a healthcare provider, this portfolio typically includes the various electronic medical records systems, ancillary clinical systems like radiology or lab systems, as well as the systems that support core business functions like human resources, billing, finance and procurement.

All of the applications in a given environment should be in compliance with licensing agreements and or enterprise contracts that validate the purchase and use of these applications by the enterprise. In this way, information services can support these applications by planning for upgrade schedules, managing their database environment, generating reports or other configuration needs from the users, and within the larger applications strategy, look to "sunset" or retire these application assets. As part of a larger security strategy, the portfolio is often assessed to drive consolidation of like-functioned applications to reduce the overall cyber or data threat surface and drive operational cost reduction for support.

In the following, these will be referenced as *sanctioned* applications, to imply that they are enterprise-owned, supported, and for the majority have been subject to a vetting or selections process by which the security posture, data flows and the primary user base of the application is known. *Unsanctioned* applications refer to those applications that are used in the enterprise that do not have direct licensing or contract or have not been reviewed by the organization. In this category are publicly published and downloaded applications off of platforms like Apple iTunes or the Android Store.

In the healthcare sector, the availability and popularity of these applications is at a tremendous growth trajectory. R2G, a Berlin-based research firm that has a dedicated mHealth Developer Economics program cites that 325,000 mobile health apps were available in 2017, with the Android store showing a 50% increase in mHealth applications from the prior year. Notably, the study also reveals that although "60% of the stakeholders in the digital healthcare are from the health industry, 40% are not from the health industry" this latter percentage is comprised of mainly tech companies, consulting companies and private agencies.[1]

[1] "MHealth Economics 2017/2018 -Connectivity in Digital Health." *research2guidance*, 2018, research2guidance.com/product/connectivity-in-digital-healt



As it pertains to mobile devices used by clinicians in the hospital setting, up until about 8 years ago when electronic medical records (EMR's) started to roll out a mobile platform rendering, the majority of applications found on personal mobile devices like tablets and phones were not visible to the organization. Currently, common technological developments like mobile device management (MDM) and network access control (NAC) are prevalent security and network access tools are used in the enterprise hospital setting. Although these solutions were initially adopted to help drive distribution of sanctioned enterprise applications to the bring-your-own device (BYOD) assets through a secure and managed method, they also provide visibility to all of the applications installed on the device. If bring-your-own-device, "BYOD", policies and

procedures do not prohibit personal mobile devices during work shifts, or an organization is not utilizing a mobile device management platform," MDM," for visibility of applications used in the environment, it is feasible and common for these mobile devices and applications to be used or referenced in the course of daily work. In some ways this is expected – phone calls, personal calendar reminders, available contact lists, personal notes and checking personal email is part of our collective daily lives. In fact, many observances have been made regarding the natural blending of our professional and private lives, and the general sense that there is a finer delineation of "life and work balance." A study presented in 2017 at the International Conference on System Science entitled "Bring Your Own Mobile Device (BYOD) to the Hospital: Layered Boundary Barriers and Divergent Boundary Management Strategies" outlines some of the challenges of increased personal mobile use in the context of the "boundary theory", used mainly in management research to explain how people enact different role identities as they transition between social domains, and typically is applied to represent changes between work and home boundaries. The study asserts that "…as these devices enter our workspaces, two key boundary concerns have emerged; the blurring of work/life boundaries, and the blurring of enterprise control and personal control over mobile use."[2]

Given current available technology, taking an enterprise inventory of these applications and analyzing the most popular used may provide important information about clinical support applications used for workflow enhancement. If those same predominant applications are not enterprise owned or sanctioned, it could be a cue for information services and / or security to take action and investigate usage. From a sourcing perspective, procurement, accounts payable

---

[2] Stephens, Keri, et al. "Bring Your Own Mobile Device (BYOD) to the Hospital: Layered Boundary Barriers and Divergent Boundary Management Strategies." *Handle Proxy*, Universidade Da Coruña, 4 Jan. 2017, hdl.handle.net/10125/41584.

and supply chain management can also help the cause. An inventory of applications that are personally expensed or purchased through departmental cost centers would also give visibility to the extent unsanctioned applications are purchased by the enterprise. In parallel with understanding the extent of use of these mobile applications in the enterprise, it is critical that analysis is conducted to understand the implication of use through the metrics of risk management. Inherent security risks associated with these applications include vulnerable code development, data integrity and overall information management. Next, we will explore the implications of "unsanctioned" application use as it relates to enterprise information security visibility and discuss potential corporate compliance concerns.

Security Risks and Privacy Implications

Many sanctioned enterprise-owned and maintained medical applications are used in the hospital environment today to support patient care and clinical and operational workflow. Mobile applications to support nurse call systems, medical engineering, catering services, electronic medical record mobile rendering, and other functions are now part of the overall information services application portfolio. Subsequently, plans for upgrades of functionality, database maintenance, and operating systems and hardware upgrades for the supporting infrastructure, as well as managing vendor risk and contracting are all under the direct supervision of the information services department. There are several security-related considerations to be made in the procurement and implementation processes of "sanctioned" applications that are entirely absent in the realm of "unsanctioned" software use. Three of the most critical concerns pertain to application level code security, data integrity, and data retention.

Software application development processes include many controls that assure usability and availability of the tool is at its optimal performance for any given user environment.

Applications analysts work continuously with their user base and the vendor to improve "click-through" flows, enable custom reporting, and maintain updated code functions to address any "bugs" or deficiencies found in the software. As it relates to security controls, analysts and software development teams keep in close communication on new security vulnerabilities discovered, and remediation steps to address security gaps. For "unsanctioned" or formally unsupported applications, these same management considerations, and attention to security attributes probably do not apply. Business drivers for data integrity may not be as relevant or personal to large development shops focused on mass-market production or distribution. Applications that are "homegrown" or developed within the medical institutions themselves, have the benefit of collaboration throughout the building process. For example, Phill Argyris , Director of Application Development and Integration for Tufts Medical Center provides some insight into the design process related to an application named CareTeam that helps with census management and care team communication. Argyris says "It took many years to get the design correct, and to figure out how they were doing their job…we built a prototype, went through information security to make sure the data security was intact, and the source repositories and other integration points maintained security controls."

In the public sector, marketplace consumers use wellness mobile health applications to help gather data on their personal health. According to an Accenture survey conducted in 2018, 75% of American consumers surveyed said technology is vital to managing health. Within the top 5 reasons for mobile services use, consumers cited using applications as reference books and tutorials, and for tracking all kinds of personal medical data. [3] These mobile applications can aid

[3] Mishra, Vikas. "Healthcare Mobile App Development Trends 2018." *Official Blog of Hidden Brains Infotech PVT LTD, Ahmedabad, India*, Accenture Survey, 8 Mar. 2018, www.hiddenbrains.com/blog/healthcare-mobile-app-development-trends.html.

everything from diabetic management, blood pressure monitoring, healthy pregnancy steps and dietary tracking. For the majority, the publishers and development sources of many "unsanctioned" mobile applications are unknown and validation of the functionality and viability of the software is unregulated by any compliance entity. Publishing and selling a mobile application on a "store" does not require outlining data sources or data flows, nor do the details of the publisher outline any secure software development lifecycle practices (S- SDLC) like validation testing or software code inspection. In Goodrich and Tamassia's textbook, "Introduction to Computer Security" the authors address that programming errors themselves may be the source of significant vulnerabilities. " …programmers should be given clear instructions on how to produce the secure system and a formal description of the security requirements should be tested against all security requirements."[4] A clear example of application development layer deficiency was unveiled recently at the 2018 Black Hat Convention in Las Vegas. Two independent researchers discovered hard-coded passwords and exposed dangerous method or function in the software supporting a Medtronic handheld patient monitor supporting an implantable heart device. Despite many documented efforts to contact the manufacturer and raise awareness to the deficiency, according to the researchers, the lack of response drove them to make the discovery public to exert pressure on the manufacturer.[5] Consistent with the current open- market mentality applied to internet commerce and use of resources, the use and applications of these resources follows a very "let the buyer beware" mentality. Unlike "sanctioned" applications, supported by licensing agreements, a bill of

---

[4] "4.4 Vulnerabilities from Programming Errors." *Introduction to Computer Security*, by Michael T. Goodrich and Roberto Tamassia, Pearson, 2017.

[5] Donovan, Fred. "Medtronic Criticized for Lax Medical Device Security Response." *HealthITSecurity*, HealthITSecurity, 13 Aug. 2018, healthitsecurity.com/news/medtronic-criticized-for-lax-medical-device-security-response.

materials which would include details about embedded and dependent code usage, and configuration specifications are not readily available.

The most prominent regulatory obligation in the healthcare industry is the Health Insurance Portability and Accountability Act, also known as HIPAA. HIPAA was enacted by Congress and signed by President Clinton in 1996 with the intent of providing guidance on the use and protection of health information and is supported through standards outlined by the Department of Health and Human Services. A related final rule pertaining to security standards was issued in February 2003 and outlines administrative, physical and technical controls to be adhered to by covered entities, or "providers" and business associates whose operations include guardianship of protected health information. With unknown entities developing and publishing mobile health applications, not only is the security of the code architecture itself a potential risk, but the probability that the functions, attributes and storage of these applications, and the adherence to HIPAA regulations is questionable. The online consortium devoted to DevOps standards information guidelines, Devops.com, addresses this frequently asked question. "If your device or application currently shares or will share the user's personal health data held in the app or device with a covered entity such as a doctor then you are dealing with protected health information and need HIPAA compliance software."[6] However, the designation of HIPAA compliance within the software profile of the Android and Apple mobile application is not required. In terms of potential clinical risk associated with an adverse clinical error related to a bug or misconfiguration, the terms within a business associate agreement (BAA) or enterprise license agreement would typically outline shared liabilities between the provider, "the user" of

---

[6] Contributor. "The Difference Between Protected Health Information and Consumer Health Information." *DevOps.com*, 10 Nov. 2017, devops.com/make-software-hipaa-complia.

the application and the application developer. For "unsanctioned" applications purchased, downloaded and potentially used for patient care, there is no recourse or method of shared liability available and formal security controls simply do not exist.

Like most mobile applications, updates and patches for these tools are dependent upon the user downloading or "pulling down" the latest version or revision from the cloud. Many times, the notes of these suggested downloads for the latest version of the application outlines that the drivers for updates have to do with new functionality, security patches, bug fixes, or updates to the software to accommodate new mobile phone operating system upgrades. In a typical "supported" application environment, the enterprise would have processes in place to test these upgrades and have quality assurance "QA" processes in place to test with the users before large scale deployment into a production environment. For personal mobile applications, this simply does not exist. As mentioned before, lack of visibility and proper management of these applications means that for all intents and purposes, the individual users are obligated to understand these terms and upgrade systems. This translates into potentially significant risk, both from an information security and potentially a clinical risk standpoint.

One of the most critical security concerns surrounding the use of publicly published "unsanctioned" mobile apps is data integrity. In the hospital setting, clinicians and care support teams use applications that can aid drug dosage conversions, census management (a clinician's assigned patient base), basic reference resources and lexicons. In an interview with Dr. William F. Harvey MD, MSc, FACR and Chief Medical Information Officer at Tufts Medical Center and Floating Hospital for Children on December 10, 2018, he suggested that "…growth charts for kids, vaccination schedules, opiod converter apps – these are examples of apps that are now popular, they are representative of apps that we put information into. Some of the most

sophisticated ones allow you to select on mild, moderate or severe reaction – it would be interesting to look at what the source information would be for these." Beyond validation of the source reference data integrity and assurance of complete, uncorrupted data though various data transmissions and translation processing is also unknown. The aforementioned lack of processes related to QA testing imply that there are minimal formal controls and "checks and balances" of the processing of data through the software, and that validation testing to consistent outcomes is not conducted. For "unsanctioned" mobile applications that store and transmit personal health data or enterprise health data, the greatest integrity risk is inadvertent corruption of the data by cyber vulnerabilities or data extraction that potentially would be unreported or unknown. When you consider the potential data corruption related to say a radiology image, a drug dosage conversion, or a reference application for allergies or drug interaction checker, the chances for error or misinformation with an openly published application on an app store, or "unsanctioned" enterprise application could have serious implications. Legal and contractual stipulations outlined in BAA agreements or enterprise-level licensing contracts mean that providers have a right to be notified in the case of a potential breach of data for "sanctioned" applications. For any other applications used or applied outside of the formal enterprise data environment, there is no mechanism or frankly the impetus for the publisher or developer to reach back out to the user to provide notification of such events. Therefore, providers and patients have no way to know whether the data has been accessed, used or disclosed in an unauthorized manner.

Finally, unless you have direct parameters around destruction, use and storage limitations, the data within mobile applications can live on in perpetuity. (This data control component is also a requirement of HIPAA). Many mobile applications rely heavily on cloud repositories and third-party processing which further distributes and proliferates data. Taking

into consideration that personal health data is at a premium for resale on the black market and dark web, these multitudes of repositories are prime targets for cyber criminals looking to capitalize on exploiting these data stores. Furthermore, given the unknown origin of publishers or creators of the data, the transfer of this information directly into data stores for direct selling is also not out of the question. In a December 11, 2018 interview with Dr. B. Scott Segel, Former Chair and Professor of Anesthesiology at Wake Forest Baptist Health, he agreed that these types of security issues were of concern. "Yes, there are security issues, do they (the user) know where the information is going, what it is used for, etc.? Who's putting in data, who has access to it and where is it going?" While this particular research project scope does not delve into privacy implications, it is widely understood that where you have unmanaged and non-permissible data use, privacy concerns are a logical parallel issue. Most recently, privacy concerns related to perceived data permissions given to third-parties has grown in public awareness with the recent Facebook privacy scandal.[7] It is not difficult then to draw the same conclusion around "unsanctioned" mobile health application use and exposure of data. As you recall, for "sanctioned" applications, there are typically controls around retention and destruction of data outlined as part of the management operations or outlined in contracts and other legal agreements that formally hold software development entities accountable. Although there are a myriad of security and privacy challenges associated with the increased proliferation of unsanctioned mobile health applications used in the clinical environment, there are some measurable advancements that can be made to advance awareness.

---

[7] Sanders, James, and Dan Patterson. "Facebook Data Privacy Scandal: A Cheat Sheet." *TechRepublic*, 2018, www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/.

Managing the Path Forward –Five Key Contributors

Healthcare Providers - Operationally, healthcare providers have the opportunity within their information technology and information security teams to identify and address the usage of these types of mobile applications in their environment. Within the last 5 years or so, many medical centers and health systems have created a new role within the leadership suite – the role of a Chief Medical Information Officer (CMIO). The creation of this role is in direct response to the acknowledgement of the rapid digitization of healthcare, and the need for an ambassador physician-trained leader to drive coordination with the technological advancements in the clinical environment. CMIO's are increasingly engaged in the clinical application and device selection process to provide influence over the investment and growth strategy of IT related to clinical services. Targeted information for CMIO's of cyber-related attributes of applications and tools would provide a critical advancement of awareness related to potential clinical or patient outcome risk tied to information security vulnerabilities and threats. Potentially, their leadership with physician colleagues and their influence as a member of hospital boards and the executive team will elevate the conversation.

Academic Medical Centers and Medical Schools - Incorporating broad high–level cyber security concepts into medical school curricula would be a logical complement to medical resident learning. "In an academic medical center, this absolutely makes sense." adds Segel. As many of the matriculated students have initial introductions into the usage of electronic medical record application technology to drive interoperability and physician/patient engagement, it seems logical and imperative to introduce this topic. In addition, more clinical service areas of study like cardiology, orthopedics, and even psychology are moving toward incorporating more electronic-enabled devices for patient care. The introduction of basic concepts like integrity and

security associated with data flow in and out of the devices would begin to bring awareness to cyber concepts as part of the initial selection and risk management process.

Medical and Ancillary Provider Associations / Organizations - Entities like the American Medical Association recognize the unique challenges associated with evaluation of a partner or vendor to support digitization and mobility of clinical processes, and to that end have published resources like the "Digital Health Implementation Playbook" which outlines considerations for security in assessing a vendor for remote patient monitoring. Within the security variables, the AMA advises to assess for "HIPAA compliance and ensuring protection of confidential patient information," and to also assess "liability and process for managing potential security breaches." Resources like these that provide a framework of key elements to assess when moving to remote or mobile application use can be refined over time to assure improvement with technological advances.

Medical society members and federal regulatory entities are increasingly acknowledging medical software application integrity, and security validity as an area of concern. Dr. Paul Summergrad, prior president of the American Psychiatric Association and the former chair of the American Hospital Association Governing Council for psychiatric and substance abuse services agrees that medical societies could provide content expertise within their body of knowledge and help with ascertaining the validity of a resource. When asked about the ability for hospital departments to coordinate conversation and awareness around unsanctioned application use in the hospital setting, Summergrad acknowledges that there are challenges in ground-level coordination and believes that societies will have a more influential role in getting the message to a broader physician base, in his words "field heads need to come together." In fact, the American Psychological Association (APA) provides an App Evaluation Model for physician

information and guidance which includes risk of privacy and security as one factor for consideration. Within the model, the APA cites that "Digital privacy and security are not often high-level risk factors when prescribing a medication or conducting in-person therapy when deciding to use an app, however, they are extremely important and should be the first area evaluated." [8]

Regulatory Agencies - Federal regulatory entities like the Food and Drug Administration are working closely with predominant medical application distribution channels like Apple to apply security controls within the design and engineering phases of some wellness applications used in conjunction with consumer health devices like the Apple watch or other Apple Health Kit offerings, but in terms of directly acknowledging a governing responsibility for the rest of the mobile health application landscape, the FDA has not been as forthcoming. Some in the industry cite the lack of direct expertise in the field of cyber security as a barrier for the FDA to directly take on the tasks of data security assurance for mobile health applications, and to some extent that is understandable given the enormity of the scope. Dr. Segel agrees, "I'm pessimistic that any regulatory body is going to help… the question is, who cares? Think about the workload involved…" With the breadth and rapid increase of developers entering this marketplace, privacy, security and integrity concerns should be top of mind for all users, direct and indirect.

Manufacturers and Developers - Like other industries, the demand for healthcare technological advancement has far outpaced the recognition of security parameters associated with mobile application software development. The blurred lines of availability and popularity of consumer-based resources with those resources and tools used in the formal clinical care

---

[8] "App Evaluation Model." *Warning Signs of Mental Illness*, American Psychiatric Foundation, 2018, www.psychiatry.org/psychiatrists/practice/mental-health-apps/app-evaluation-model.

setting can pose a challenge in many ways. Integrity concerns with unknown source data and implications of data corruption due to software vulnerabilities or 'bugs' has not yet risen to the forefront of issues to be addressed, yet the risk potential is clear. Currently, medical device vulnerabilities are making headlines in terms of understanding cyber risk and potential effect on patient care, and most technologists understand that the crux of the issue lies in software coding deficiencies and the potential lack of security controls of the supporting network. This problem is more readily addressable by working with manufacturers of the devices and with network engineers – two parties accountable to the quality and security of the product. For mobile health applications freely published and distributed in open marketplaces, there is little accountability or recourse for a quality standard. In this case, the Food and Drug Administration (FDA), American Medical Association (AMA) and the National Cybersecurity Administration (NSA) should collaborate to form an advisory committee to provide guidance for awareness campaigns in the public and private sector. This triumvirate power is also in the best position to draft legislation for standards and obligatory safety ratings for these applications on the open market that can be published alongside popularity and download metrics on the application store postings.

Finally, given my unique personal experiences and current professional focus, there are next steps which I can take to influence change and escalate awareness. Targeted distribution of the published version of this report can be shared with key leaders in the above five areas to start conversations around tactical next steps to help reduce risk pertaining to mobile medical device use. I can use this CCP and presentation as an outline to speak at industry events and forums that have a vested interest in this topic, such as the College of Healthcare Information Management Executives (CHIME) and Healthcare Information and Management Systems Society (HIMSS). I

can raise awareness by being a guest speaker or presenting to the Brown Executive Master's Program of Healthcare Leadership, and other entities like these, and offering to speak with the dean of the medical school. Contributing a summary of this study as an Op-Ed piece to periodicals like the American Medical Association (AMA) and the New England Journal of Medicine (NEJM) will also help to drive industry awareness and fulfill a personal goal I considered when choosing a topic for this assignment. Lastly, in my current professional capacity, I am frequently asked to speak on panels addressing various facets of information security program challenges, including medical device security. (I was recently on a panel with a policy coordinator of the FDA) I can continue to use these forums which are transcribed, posted and published by media outlets to drive thought leadership within my own professional circles.

As recounted in my personal narrative, the use of mobile health applications can be surreptitious and unknown to the enterprise but have a favorable result in expediting or simplifying care. Unfortunately, the use or application of mobile tools may also have the opposite effect causing adverse risk to clinical care; as we have reviewed, this scenario would be relatively undocumented or auditable in the formal medical record. Investments in information technology and security infrastructure at the enterprise level is helping to address the visibility problem, but policy development and culture need to be acknowledged as critical support methods. Although regulatory entities, medical societies, and even higher education institutions are increasingly recognizing the potential security and privacy risks associated with these complex technologies, there is still a fair amount of work to be done, and all parties seem to agree that the vast enormity of the problem is one of the largest hurdles.

APPENDIX A: Bibliography

"4.4 Vulnerabilities from Programming Errors." *Introduction to Computer Security*, by Michael T. Goodrich and Roberto Tamassia, Pearson, 2017.

"App Evaluation Model." *Warning Signs of Mental Illness*, American Psychiatric Foundation , 2018, www.psychiatry.org/psychiatrists/practice/mental-health-apps/app-evaluation-model.

Arista, Sonia, and B.Scott Segel. "CCP - Clinician Interview ." 11 Dec. 2018.

Arista, Sonia, and Paul Summergrad. "CPP - Clinician Interview." 17 Dec. 2018.

Arista, Sonia, and Phill Argyris . "CPP - IT Operational Interview." 17 Dec. 2018.

Arista, Sonia, and William Harvey . "CCP - Clinician Interview ." 10 Dec. 2018.

Contributor. "The Difference Between Protected Health Information and Consumer Health Information." *DevOps.com*, 10 Nov. 2017, devops.com/make-software-hipaa-complia.

Donovan, Fred. "Medtronic Criticized for Lax Medical Device Security Response." *HealthITSecurity*, HealthITSecurity, 13 Aug. 2018, healthitsecurity.com/news/medtronic-criticized-for-lax-medical-device-security-response.

"MHealth Economics 2017/2018 -Connectivity in Digital Health." *research2guidance*, 2018, research2guidance.com/product/connectivity-in-digital-health/.

Mishra, Vikas. "Healthcare Mobile App Development Trends 2018." *Official Blog of Hidden Brains Infotech PVT LTD, Ahmedabad, India*, Accenture Survey, 8 Mar. 2018, www.hiddenbrains.com/blog/healthcare-mobile-app-development-trends.html.

Sanders, James, and Dan Patterson. "Facebook Data Privacy Scandal: A Cheat Sheet." *TechRepublic*, 2018, www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/.

Stephens, Keri, et al. "Bring Your Own Mobile Device (BYOD) to the Hospital: Layered Boundary Barriers and Divergent Boundary Management Strategies." *Handle Proxy*, Universidade Da Coruña, 4 Jan. 2017, hdl.handle.net/10125/41584.

APPENDIX B: Other Sources

Industry Conferences

- HIMSS (Healthcare Information and Management Systems Society) 2018 Healthcare Security Forum - October 15 -16, 2018 – Boston, MA
- HIMSS 2018 (Healthcare Information and Management Systems Society) Big Data and Healthcare Analytics Forum – October 22-23 – Boston, MA
- CHIME (College of Healthcare Information Management Executives) FALL CIO Forum – Oct 30 – Nov 2 – San Diego, CA
- NH-ISAC (National Health Information Sharing and Analysis Center) Fall 2018 Summit – November 26-30 – San Antonio, TX

Other Media and Periodicals

MA Data Health Consortium – "The Internet of Medical Things: Optimizing Security and Effectiveness" Webinar September 12, 2018

Personal Industry Contributions

Medical Devices: The Long Road to Security- Healthcare Information Security Media Group – Interview November 21, 2018 - https://www.healthcareinfosecurity.com/medical-devices-long-road-to-security-a-11718

Healthcare IT Teams Need to Proactively Address New Cyberthreats Trends – Interview November 19, 2018 - https://www.hitechanswers.net/healthcare-it-teams-need-to-proactively-address-new-cyberthreat-trends/

Healthcare IT News – "Healthcare infosec leaders rank security posture, maturity just 'average'" – Panel October 16, 2018 - https://www.healthcareitnews.com/news/healthcare-infosec-leaders-rank-security-posture-maturity-just-average