ICIT - Institute for Critical Infrastructure Technology

Preventative Measures: Ensuring Information Security Prior to mHealth Development

The "generation, aggregation, and dissemination of healthcare information via mobile and wireless devices", known as mHealth, is poised to disrupt the current state of global healthcare as drastically as the 1990's disruption of the technology sectors caused by the emergence of the internet. Efficient application of mobile healthcare presents a win-win solution for the users and providers who benefit from decreased operational costs, wider outreach, and innovation. However, careless implementation of mHealth applications without proper consideration of security and privacy could harm users, cost billions, and forever taint successful advancement in the healthcare sector. Like the internet, an effective collaboration between the Federal government and non-federal entities can maximize the positive impact on users by significantly increasing the utility of mHealth while minimizing the risk to users by limiting the threat landscape.

Mobile healthcare applications allow users to submit and obtain personal healthcare information on any wireless device, in real time. The widespread adoption of a mHealth framework would allow many seniors the ability to remain in their homes, with loved ones, rather than in care facilities. Moreover, chronic diseases like asthma, obesity, and diabetes account for ~46% of the global disease burden and mHealth applications provide convenient monitoring of chronic indicators. Access to the internet is the only thing a patient requires to report an incident, track their condition according to their indicators, or discuss symptoms and treatment with trained physicians. Mobile healthcare connects patients with providers, regardless of physical location; thereby, providing an optimal solution to healthcare in which quantity of needed assistance can exactly match the supply of expertise. Patient health is monitored more frequently, at less financial and temporal burden to physicians. Data can be aggregated and analyzed with greater precision to yield innovative research. This is especially inspiring in areas of mental healthcare, such as treatment of depression, where real time data are rare and treatments vary significantly. Applications enable patients to report as symptoms occur so that researchers can better understand the condition and develop treatment that is more effective. Medication effectiveness can be regularly surveyed amongst patients and ineffective treatment can be discontinued. The economic and physical well-being of the entire world can greatly benefit from efficient implementation of mHealth technology. Despite the benefits, improper implementation of mHealth could leave users at great risk. Digital records must be secured from infinite avenues of attack. Patient security and privacy can be maintained on a mobile platform if many of the security controls utilized in large hospitals are applied to the application level and user process of the mobile platform. It is critical that the initial adoption of mHealth properly ensures the protection of sensitive information and the protection of patient privacy.

Personal healthcare information (PHI) is estimated to be up to ten times more valuable to cyber-attackers than credit card information; however, it is often easier to obtain through cyber-attacks or social engineering. Cyber-attacks on the healthcare industry have increased over 125% in the last five years. The resulting breaches cost providers ~$6 billion annually without considering the cost to the patients whose identities were compromised in the attacks. The healthcare industry has recently realized the value of regular risk analysis through iterative processes such as CERT's OCTAVE Allegro, or a comparable methodology, which help to define the attack surface, determine risk appetite, and determine the critical assets at risk. Because the cost to update outdated systems to secure PHI from attackers grossly outweighs the $1.5 million annual maximum penalty due to HIPAA violations, many healthcare providers accept the risk of exposing patient records due to a breach. As a result, the impact of the breach unjustly affects consumers. As mHealth becomes ubiquitous, breaches become more viable and more profitable. Measures to secure sensitive data and ensure patient privacy must precede the adoption of mHealth applications else, consumer data will be at significantly greater risk. Security cannot be an afterthought in mobile healthcare. It is the responsibility of the federal government and non-federal entities alike to ensure that users are not crash test dummies for insecure healthcare applications. Defining clear liability conditions and increasing the penalties associated with healthcare breaches would compel providers to invest more in system resiliency to preclude breaches.

One of the primary ways of deterring a breach is to reduce the value of the target. If federal regulations and standards compel mHealth providers to improve security, then the value of healthcare data decreases because attackers must invest greater resources to breach a system. The federal government and non-federal entities can inspire improved system resiliency by promoting data centric models that focus on decreasing the value of a breach by increasing the difficulty of obtaining useful data. This is predominantly achieved through encryption of the data or through hash functions. According to notable security blogger Brian Krebs, many of the healthcare systems that employ data centric models currently undermine their efforts by employing weak encryption or outdated hash functions, such as SHA-1 or MD5. Stronger encryption, such as 256 byte AES, and the strong SHA-2 hash function should replace weaker models where possible. However, since encryption strength is often proportional to the length of the key and the processing time of the algorithm, data centric models may not suit all mHealth applications. A balance must be established between the strength of the encryption and the acceptable processing time to access stored data. Given the vital circumstances for legitimate access to personal health information, time may be a critical factor. Further, encrypted data are still valuable to a patient attacker because personal health information can retain value for decades. As Moore's law predicts computing power to increase exponentially each year, sufficient encryption will likely be idle work in a few years.

The increased use of mHealth data in the United States medical delivery system will increase the need for security and privacy controls. A more comprehensive, defense-in-depth model can ensure that a data centric approach does not lead to a false sense of security. One prominent model involves creating a 3x3 matrix to ensure that the confidentiality, integrity, and availability of data are maintained wherever data are stored, transported, or processed. This model ensures that the provider knows where data are stored and that the site is as secure as possible. PHI should not be stored on cloud servers unless the company assumes greater liability. The model encourages companies to establish patient authentication, data recovery, and data loss requirements to ensure availability. Policies minimizing shared information to necessity enforce the confidentiality requirement. Adoption of redundant servers and auditing reinforces data integrity. Federal and non-federal entities can increase the adoption of defense in depth models through regulation or through best practice training programs.

The decision to impose regulations or to initiate training programs depends upon the situation, the desired goal and the targeted market segment. The movement towards digitized medical records can cause public panic. However, if security and privacy controls are ensured prior to the transition, then the resulting networks will likely be more efficient and more resilient to cyber-attacks and insider threats. It is notable that many large hospitals such as UPMC have recently implemented many of the security procedures mentioned; however smaller hospitals must be as responsible as large hospitals to prevent data breaches at the weaker link. The federal government may wish to impose regulations to assuage the fear surrounding mHealth adoption. Citizens also deserve clear definitions of the types and legal uses of shared PHI. Furthermore, since hospitals adopted electronic health record (EHR) systems at different times, a federally established standardized mHealth platform, format, and/ or framework would mitigate the risk associated with mismatched provider frameworks and the physical risks from fax machines and insider threats that accounts for many cases of identity theft. Federally established guidelines detailing rights to access personal data or the personal data of someone in a user's care (delegation of trust model) would also be necessary so that all providers uphold the same policies. Users also benefit from compliance regulations mandating replacement of outdated systems, regular updates and patches of systems, and unambiguous timeline for reporting a breach to the government and consumers. The federal government may also want to mandate certain security features to ensure the protection of users. Multifactor identification through biometrics, digital identification, or physical technology, significantly reduces unauthorized access to data. An alternate route, suggested by ICIT Fellow and HP Security Strategist Cindy Cullen, would be to mandate or incentivize mHealth devices with hardware root of trust. Even if an actor manages to access PHI through the internet, hardware root of trust ensures that only trusted devices can access data. Enterprise monitoring and mobility solutions can ensure that the correct patient receives the correct records. Enterprise level logging ensures that providers can be regularly audited in the event of a breach or civil suit. Finally, the federal government has the resources to sponsor training programs to inform patients, doctors, and providers of the best practices to protect security and privacy.

The federal government or non-federal entities could also sponsor CISO training programs that teach IT personnel to focus on information security. Because healthcare providers and doctors focus on providing timely healthcare, improved long -term security culture may be best achieved by training dedicated personal. Trained personal could serve as CISO's, contractors, or consultants. Non-federal entities are specifically well placed to sponsor training programs capable of changing the security culture in the healthcare sector as mHealth adoption increases. According to ICIT Fellow Clinton Racine, "a doctor's primary goal is caring for their patients. Because change in their workflow can distract from this primary goal doctors are reluctant to adopt new software and technology. So, business administrators and the IT staff must make every accommodation possible so that doctors can incorporate new technology without interrupting their workflow. Convincing a doctor with 30+ years of experience to adopt new technology when seeing a patient is a difficult task made far easier when administrators, IT and other staff prioritize the doctor's primary goal: seeing the patient." Non-federal entities such as contractors and technology developers can train users upon distribution of the technology, as part of the purchase agreement, without disrupting the workflow of healthcare providers. As a result, Doctors and administrators would receive training through many of the same channels used when a hospital purchases a new technology, such as a new MRI. Non-federal entities are also better suited to assist small businesses who lack the training to handle PHI. Finally, non-federal entities can train their own employees and the employees of other firms to implement security and privacy controls throughout the application development process. This ensures that companies test security features for vulnerabilities prior to consumer adoption. Non-federal entities greatly benefit from establishing and disseminating practices to regularly measure the accuracy of mobile health monitors because private entities are the most likely beneficiaries of the big data resulting from mHealth monitors.

The federal government, non-federal entities, and healthcare providers must ensure that patients understand what information is shared, stored, and used. The federal government may want to preempt legal battles by regulating whether Healthcare IT firms, healthcare providers, or patients retain proprietary rights to PHI. The federal government must also decide the distribution of liability, sans SLA, between healthcare provider and healthcare IT firm, in the event of a breach because consumers have the right to know who is responsible for compromised data. As with the internet, as users understand how their information travels through the network and they acclimatize to mHealth best practices, a long-term culture of security will spread. Due to a disparity in technical knowledge in the population, senior citizens are one of primary target groups of cyber-attacks and social engineering. Because a large percentage of mHealth users will be elderly, effective user training is imperative. Training must be clear and informative. Covenant Security Solutions Inc. President and Founder Danyetta Fleming Magana recommends hosting training programs for senior citizens at "grassroots" locations such as churches, activity centers, and schools to increase effectiveness. Alternately, the federal government could disseminate targeted training programs through the Center for Medicare and Medicaid Services (CMS), through the Department of Health and Human Services (HHS), or through collaboration with national health advocacy groups. Regardless of technical proficiency, clarity of rights and information usage is more important than precision. Patients deserve the right to understand the informed consent that providers request, more than they need to know every technical detail. Furthermore, in depth descriptions of how information security to an untrained audience may lead to misleading statements or unrealistic expectations of security. Jargon and technical details should not obfuscate how information travels through mHealth networks.

Patients and healthcare providers will need the federal government to amend title II of H.R. 1560 to provide direct language detailing the usage of PHI by DHS or the NSA if such information needs to be shared. Neither title of H.R. 1560 specifies a need or desire of shared PHI, however a breach in the healthcare sector could necessitate such a transfer. In all likelihood, the Healthcare ISAC will prohibit the transfer of PHI to the NCCIC as a liability protection against civil suits. Moreover, since PHI is mostly PII, the two data scrubbing processes mandated by H.R. 1560 would preclude any meaningful data transfer.

The emergence of mobile healthcare capabilities can forever alter how users provide and receive healthcare in the United States. Mobile Healthcare will continue to emerge and develop, whether or not user security and privacy is considered. As mHealth becomes ubiquitous, the federal government and non-federal entities must ensure that the market disruption yields effective security and privacy controls, a transparent mHealth network, and a more security conscious population else, the healthcare sector will succumb to data breaches that will significantly impact the lives of millions of citizens. Through a security driven focus, clear communication, and effective user training, the adoption of mHealth will significantly improve healthcare for every United States citizen without putting their lives at risk.

*Expert research contributed by the following ICIT Fellows:

- James Scott (ICIT Senior Fellow – Institute for Critical Infrastructure Technology)
- Drew Spaniel (ICIT Visiting Scholar, Carnegie Mellon University)
- Rob Roy (ICIT Fellow – Federal Chief Technology Officer, U.S. Public Sector, HP)
- Cynthia Cullen (ICIT Fellow - Security Strategist, Northeast, HP)
- Stan Wisseman (ICIT Fellow - Security Strategist, Southeast, HP)
- Chris Schumacher (ICIT Fellow - Sr. Technology Consultant, New Light Technologies)
- Dan Waddell (ICIT Fellow - Director, Government Affairs, (ISC)2)
- Daniel Skinner (ICIT Fellow – Chief Product Officer, Watchdox)
- Danyetta Magana (ICIT Fellow – President & Founder, Covenant Security Solutions)
- Clinton Racine (ICIT Fellow – Co-Founder, ELXR Health)
- Paul Emmanuel (ICIT Fellow – Co-Founder and CEO, ELXR Health)
- Morgan Muchnick (Director of Legislative Affairs, Institute for Critical Infrastructure Technology)

American Medical Association (AMA)

http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page

CIO Enterprise Forum

http://www.enterprisecioforum.com/en/blogs/hp-security-strategists/securing-your-data

Deloitte Consulting

http://www2.deloitte.com/us/en/pages/life-sciences-and-health-care/articles/center-for-health-solutions-networked-medical-device-cybersecurity-and-patient-safety.html

Greatcall Infographics

http://www.greatcall.com/lp/is-mobile-healthcare-the-future-infographic.aspx

Healthcare Information Management and Systems Society (HIMSS)

http://www.himss.org/library/mhealth

http://www.himss.org/ResourceLibrary/genResourceFAQ.aspx?ItemNumber=36890

mHealth

Prasad, Aarathi, et al. "Understanding User Privacy Preferences for mHealth Data Sharing." *mHealth* (2014): 545. Web

PWC

http://www.pwc.com/gx/en/healthcare/mhealth/#&panel1-1

Sans Institute

https://www.sans.org/reading-room/whitepapers/analyst/threats-drive-improved-practices-state-cybersecurity-health-care-organizations-35652.

Science

Estrin, Deborah and Sim, Ida. “Open mHealth Architecture: An Engine for Health Care Innovation.” Science. (5 November 2010): 330 (6005), 759-760.Web.

The VAR Guy

http://thevarguy.com/network-security-and-data-protection-software-solutions/051415/study-cyber-attacks-cost-healthcare-industry

United States Government Accountability Office

http://www.gao.gov/products/GAO-15-319