Cybersecurity and Home Health: Adaptations to a Growing Issue

Timothy Kwong

ENLC 556

University of San Diego

Cybersecurity and Home Health: Adaptations to a Growing Issue

Being in the middle of the technological age we can only wonder where the next 5 years will lead us, even the next 10 to 15. Technologies and methods in healthcare have been changing at such a rapid pace that it is hard to keep up with. There has been a trend in allowing patients to be able to monitor their health at home, whether it be a singular medical device or through an application monitoring basic vital data on their health to report to their primary care doctor. In the midst of our current pandemic the use of telehealth has seen its slow adoption all the sudden skyrocket without the infrastructure necessarily to support it. With the plethora of technologies available to health care practitioners and patients alike it leaves a very large opportunity for malicious attacks.

Health information is very valuable to patients and their caretakers, with electronic health records taking center stage in pretty much any modern healthcare system they are vulnerable to cyber attacks. It has been a long standing issue that hospitals and health systems are dealing with on a constant basis. Now that health care technology has tried to adapt to the modern age we see the huge growth of health technologies in the home. The use of sending diagnostic data from medical devices from the comfort of the home so that the patient does not need to go into the clinic has provided leaps and bounds for convenience to both sides of the health care team. In todays age the use of social media platforms has led the countless adoptions of the use of those platforms to share health information and thus leaving those platforms vulnerable to cyberattacks.

Kramer & Fu (2017) mention that the Food and Drug Administration had found that pacemaker devices were found to have their batteries compromised to malware that could affect the function of those devices made by St. Jude. This led to around 450,000 patients that had their health compromised and new updates needed to be given to those devices. This leads to patients in fear for their lives and hospitals/clinics needing to spend time and resources to fix the issue. Not only is healthcare compromised but organizations are put in a very rough spot for not being able to properly protect their patients. With the inevitable growth and use of technology in the home setting more needs to be addressed to see where its vulnerabilities are and how to deal with the issues present and the issues that will inevitability come. If organizations want to meet the needs of the consumer and be able to do so safely they need to make it a priority to address those alarming issues as if they are already present.

Addressing the increasing vulnerabilities of health care information and internet security in the home-based health care realm is very important to enable the platform to have longevity and continually get better. Ranging from transmission of health care information to the end-user protecting their own health information when using these applications at the home there is a very diverse approach to protecting that data.

Williams and Woodward (2005), had investigated the intricacies of protection of networks and medical devices. With the increasing of the use of networks to transmit data from home through implanted medical devices there has been a worry of vulnerabilities that they would face. As we know the more networks that are involved with data transfer the greater the risk of an attack on that information. They discovered it is not necessarily as simple as protecting the device or the networks involved. It is a very complex system to which everything has to work in collaboration and feed off of each other. Device manufacturers, IT departments, and health

care practitioners need to work together to protect that information they are trying to use to help their patients. The complexity has to do with each device being proprietary so there is no one size fits all solution. Every time there is a software update it must go through regulatory boards and to be approved for the market and thus new software to protect its operations. There was the creation of the FDA Safety and Innovation Act to try to get companies and organizations to become more proactive to protect the networks and devices themselves for patient safety but has been a slow uptaking. In the end it is an effort where expertise from all departments, regulations and standards must be set proactively, not individual departments working on their own goals.

Henriksen et al. (2013) ran a risk assessment study in home-based platform for chronic disease rehab and education, in their study evaluating chronic obstructive pulmonary disease and diabetes. They conducted the study by evaluating security measures of confidentiality, integrity, availability and quality. In their risk assessment methods they state they impossible to completely avoid any risk (zero), hard to define what level of risk is acceptable, especially in the healthcare information field. They determined that confidentiality breach is the highest risk level and deemed a catastrophic failure of the home-based system. With their assessment 1 out of the 50 breaches they detected was deemed catastrophic due to third-party access to health information on TV screen, this was dealt with by creating barriers to keep it from happening. In this case they implemented a time-out procedure when system was left idle for set amount of time and patient was not interacting with the system.

Cybersecurity should be addressed in both pre- and post-market product testing. Firmware updates to patch known vulnerabilities in current on-market devices. Remote interrogations of cardiac implant devices. Right now, there is not much evidence of hackers being able to reprogram individual devices but rather the communication networks between

hospitals and the end-users. Inhibition of telemonitoring for cardiac events. However, if hackers are able to truly change settings this can become life threatening especially in AICD devices or pacemakers, such as oversensing and causing more shocks to reset heart rhythm or even life-threatening ones (Baranchuk et al., 2018). Physicians and medical device companies need to be on top of vulnerabilities as well as communication losses that they are able to detect. Government involvement with FDA and creating regulations for these cardiac devices to address. Being proactive in potential cyber security issues need to be handled immediately whether it be through firmware updates or communication with patients to have device managed in clinic.

With more and more people using social media platforms daily there has been the rapid development of health care applications for users. This starts to pose a risk for breach of health information and invasions of privacy Al-Muhtadi et al. 2017 took at look at potential solutions to address these issues that will undoubtedly arise from the use of such applications. Having designated users that will have access to certain information is the main way it is discussed to protect information to make it secure on such networks. It also depends on the end-user to protect that information properly as well, not just relying on the actual application to protect the information and proper training and education should be conducted.

Solutions yielded from these studies shows the complexity of dealing with protecting health information in the modern technology age. As with the further development of these home-based health technologies being proactive in predicting vulnerabilities needs to addressed as well and immediately remedying current problems arising.

To address the issue of software and device vulnerabilities we need to take a closer look at the way different organizations that work to help the patient: hospital, device manufacturer

and government regulatory board (Food and Drug Administration, FDA). All three of these large entities that work to get these devices in patients to help them need to understand that it is a collaborative effort to ensure the safety of the patient. If all work individually there can be lapses in their protective effort and thus put the patient at risk thus the organizations themselves as well.

Medical devices themselves have regulatory boards but there is no oversight when it comes to cybersecurity management (Ransford et al. 2017). FDA recommends implementing a proactive comprehensive cybersecurity risk management program. Including monitoring cybersecurity information sources (common vulnerabilities and exposures), robust software lifecycle processes, assessing and detecting presence and impact of vulnerabilities, definition of communication processes for vulnerability intake and handling, using threat modeling on a regular basis, adopting a vulnerability disclosure policy and practice, deployment of mitigations that address cybersecurity risk early and prior to exploitation (Lechner, 2017).

Providers can take initiative by adopting the “industry standards for cybersecurity and ensuring that procurement practices treat these standards’ prescriptions as requirements” (Ransford et al. 2017) As of today there have not been any real threats to remote medical device management where it could potentially threaten the life of the patient. However, it is highly advisable that precautions be taken for the chance of something fatal happening in terms of cybersecurity flaws in medical devices. As seen from literature review, there needs to be more collaboration for all entities involved with the devices as to ensure all involved are confident enough to allow their patients to have these devices supporting their health without jeopardizing it.

A failure mode effect analysis (FMEA) looks at the inevitability that there will be a failure down the line for the cybersecurity of the device or the security integrity of the device

itself. We look at the possible areas where these vulnerabilities can happen as shown through the flow chart as well as detailing those steps and possible remedies, but is definitely a fluid situation.

Figure 1

Failure Mode and Effect Analysis (FMEA)

Step	Potential Failure Modes
1	- Patient unaware of communication failure - Device unable to alert user of communication failure - Home clinic unaware of communication failure and fails to alert patient putting patient's health at risk
2	- Loophole identified but time frame too long putting device and patient at risk - Different hardware models for same device potentially delaying software patch - New loopholes develop
3	- Patient unable to link device to receive update, communication failure - Unable to physically travel to clinic to have firmware updated - Firmware patch causes issues and has bugs that causes more issues
4	- Patient unable to go into clinic, may live very remote - Technician not trained properly or unavailable when patient is available to come for interrogation - Time for training clinics for proper interrogation, software deployment
5	- By time firmware with cybersecurity patch is installed new malware or attacks may have happened - Unable to link device, or older devices may not be compatible, need multiple versions of patch to address different hardware requirements

	- May need physical link to device to install firmware update

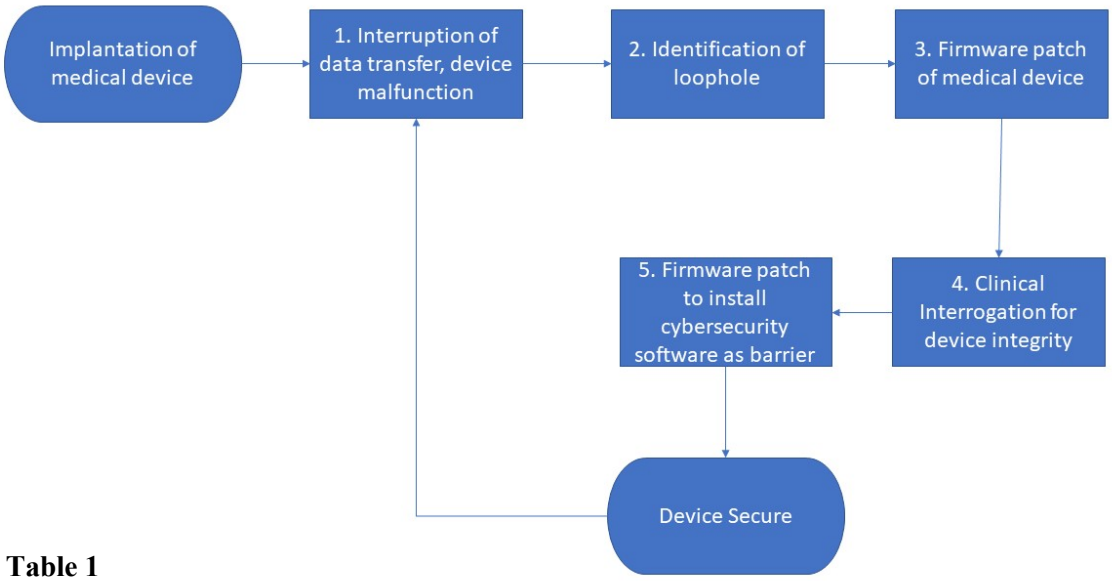

Table 1

FMEA Steps potential failure modes

FMEA Process Steps

Table 2

Process Step #1	**1**	**Process Step**	Interruption of data transfer, device malfunction		
	2	**Potential Failure Mode**	Patient unaware of communication failure	Device unable to alert user of communication failure	Home clinic unaware of communication failure and fails to alert patient putting patient's health at risk
	3	**Potential Cause(s)**	Patient not trained properly on how to use device/connect	Faulty device, not interrogated correctly, problem not corrected	Clinic staff not trained properly to keep up on all active patients on days to be reported
	4	**Severity**	2	2	3
	5	**Probability**	Frequent	Uncommon	Uncommon
	6	**Hazard Score**	4	3	3
	7	**Action (Eliminate, Control, or Accept)**	Control	Control	Eliminate

	8	**Description of Action**	1. Train patient on connectivity software 2. Give information to patient on what to look for, contact information 3. Training patient to contact when issues occur	1. Frequent device interrogation 2. Periodic device updates from clinic 3. Firmware updates when manufacturer is aware of issue	1. Frequent communication with patient 2. Establish contact with patient (hotline) 3. Weekly audit of active patients

Table 3

Process Step #2	**1**	**Process Step**	Identification of loophole		
	2	**Potential Failure Mode**	Different hardware models for same device potentially delaying software patch	Different hardware models for same device potentially delaying software patch	Home clinic unaware of communication failure and fails to alert patient putting patient's health at risk
	3	**Potential Cause(s)**	Manufacturer making different versions of same product due to longevity of certain devices	Manufacturer making different versions of same product due to longevity of certain devices	Clinic staff not trained properly to keep up on all active patients on days to be reported
	4	**Severity**	4	4	3
	5	**Probability**	Remote	Remote	Uncommon
	6	**Hazard Score**	2	2	3
	7	**Action (Eliminate, Control, or Accept)**	Accept	Accept	Eliminate
	8	**Description of Action**	1. Give option to patients to install new device so patch deployment not as complicated 2. Develop firmware patches for all models on market 4. Make sure all models addressed as soon as software available	3. Give option to patients to install new device so patch deployment not as complicated 4. Develop firmware patches for all models on market 4. Make sure all models addressed as soon as software available	4. Frequent communication with patient 5. Establish contact with patient (hotline) 6. Weekly audit of active patients

Table 4

Process Step #3	**1**	**Process Step**	Firmware Patch of Medical Device		
	2	**Potential Failure Mode**	Unable to physically travel to clinic to have firmware updated	Unable to physically travel to clinic to have firmware updated	Home clinic unaware of communication failure and fails to alert patient putting patient's health at risk
	3	**Potential Cause(s)**	Patients live remotely from primary location to install software	Patients live remotely from primary location to install software	Clinic staff not trained properly to keep up on all active patients on days to be reported
	4	**Severity**	2	2	3
	5	**Probability**	Frequent	Frequent	Uncommon
	6	**Hazard Score**	4	4	3
	7	**Action (Eliminate, Control, or Accept)**	Accept	Accept	Eliminate

	8	**Description of Action**	1. Travel to patient home to help with software installation 2. Pay for patient transportation to clinic 5. Develop remote patch until patient can come to clinic	3. Travel to patient home to help with software installation 4. Pay for patient transportation to clinic 5. Develop remote patch until patient can come to clinic	7. Frequent communication with patient 8. Establish contact with patient (hotline) 9. Weekly audit of active patients

Table 5

Process Step #4	1	**Process Step**	Clinical Interrogation for device integrity		
	2	**Potential Failure Mode**	Patient unable to go into clinic, may live very remote	Patient unable to go into clinic, may live very remote	Home clinic unaware of communication failure and fails to alert patient putting patient's health at risk
	3	**Potential Cause(s)**	Patient lives in a remote location, only comes to clinic when absolutely necessary	Patient lives in a remote location, only comes to clinic when absolutely necessary	Hackers discover new loopholes that may not have been patched before
	4	**Severity**	2	2	4
	5	**Probability**	Frequent	Frequent	Uncommon
	6	**Hazard Score**	4	4	2
	7	**Action (Eliminate, Control, or Accept)**	Accept	Accept	Accept
	8	**Description of Action**	1. Provide alternative transportation 2. Technician to travel to patient site 3. Create remote upload of software patch	1. Provide alternative transportation 2. Technician to travel to patient site 3. Create remote upload of software patch	1. Anticipate that loopholes will be discovered in software 2. Do annual software patching to address loopholes or new cybersecurity 3. Immediately address loopholes rather than waiting for incident to occur

Table 6

Process Step #5	1	**Process Step**	Firmware Patch to Install Cybersecurity Software as Barrier		
	2	**Potential Failure Mode**	By time firmware with cybersecurity patch is installed new malware or attacks may have happened	Unable to link device, or older devices may not be compatible, need multiple versions of patch to address different hardware requirements	May need physical link to device to install firmware update
	3	**Potential Cause(s)**	Delay in developing software patch	Needing multiple versions of software for all device versions	Original software did not have option programmed in
	4	**Severity**	7	7	4
	5	**Probability**	Uncommon	Uncommon	Uncommon
	6	**Hazard Score**	6	6	4

	7	**Action (Eliminate, Control, or Accept)**	Accept	Control	Eliminate
	8	**Description of Action**	1. Fast deployment of temporary patch 2. Loopholes and attacks should be anticipated, when loophole detected address immediately 3. Have basic infrastructure of code laid out with patches added on when vulnerability is known	1. Have all device versions on market addressed at same time with patches in timely manner 2. Know all versions and their requirements 3. Personnel trained in all areas and versions that will be deployed	1. With new firmware address physical link issue 2. Have new devices that can be remotely managed 3. Have patient to come into clinic for updates

Quality Measure Plan

In terms of quality measures, we will be using the Plan-Do-Study-Act (PDSA) cycle tool to measure and reassess quality improvement for the management of cybersecurity with our home medical devices. It can be applied to all medical devices in general as all have some vulnerabilities and individual devices may have some specifics, but the initial approach and response should be similar. The PDSA allows us to address each measurement individually and evaluate process measurements to reach the eventual goal of our outcome measurement of tackling cybersecurity for home medical devices overall. For the first measurement from our FMEA we look at communication interruption and device malfunction. To address this, we need to get feedback from both patients as well as clinical staff on finding what the main issues were and tackling those issues. For example, did patients feel they were adequately trained to use devices from home or communication with clinical staff appropriate to resolve issues or did we see issues on both ends. If we find which is the common factor, we address that first then see what the changes come from that change. Data will be collected in the form of transcribing calls in patient-clinical staff interactions. From the interactions staff can create table of most common issues to come up with solution. The outcome process desired is to decrease the calls in general as well as technical issues due to not knowing ecosystem.

The next few measurements are all technical aspects of the cybersecurity of the home health devices. First the of the identification of the loophole will lean more towards the IT team as well as the device manufacturer. Loopholes will usually be detected from the previous measurement exposing it, however annual audits of the program itself can help avoid problems like it from occurring as well. Following this measurement will be the development of the firmware patch which will be done through manufacturer. One measurement we can make is a process measurement of the patient being able to communicate with the manufacturer or clinical staff to establish device link and enable smooth transition of update installation. The clinical manager or IT manager can be the one monitoring the outcome of the performance measure. They will measure how many successes they have on first time link establishment and installation versus how many devices they needed to troubleshoot or have physical management. Device integrity as well as final patch with cybersecurity software installed will fall on similar lines to establish performance outcomes and determine if intervention is needed and when intervention is done if it improves future outcomes. Running data from previous years and tickets that were issued to deal with those problems will be used to compare with intervention program that is developed from the PDSA and we will be able to see if the program has a positive or negative effect on the desired outcome of dealing with the FMEA issues head on.

Using a PDSA with feedback from staff as well as patients will help create a successful quality improvement process especially in the early stages of FMEA measurements. Early intervention will ensure smoother process and better outcomes down the line of measurements. If they know the problem exists, they can intervene and prevent catastrophe. It comes down to communication between provider, device manufacture and end user (patient) to truly create better QI outcomes for the home medical device and its cybersecurity.

When it comes down to cybersecurity vulnerabilities in home health devices there needs to be a holistic approach to its safety and ultimately patient safety. When there is a conscious effort put bring all sectors involved with the product development, implementation and patient care then they can be at the forefront of protecting the device as well as the patient at the same time. Cybersecurity issues will happen no matter how well the device is developed. Anticipating that the issue will occur needs to be addressed, while at the same time developing a device that can deal with those issues from the start is of equal importance. The current landscape there is no regulation of cybersecurity or requirement in devices for home health and that is alarming. Addressing the needs both in the regulatory boards as well within organizations is the first key to get the ball rolling and provide better protection and outcomes for all involved.

References

Al-Muhtadi, J., Shahzad, B., Saleem, K., Jameel, W., & Orgun, M. A. (2017). Cybersecurity and privacy issues for socially integrated mobile healthcare applications operating in a multi-cloud environment. *Health Informatics Journal, 25*(2), 315-329. doi:10.1177/1460458217706184

Baranchuk, A., Refaat, M. M., Patton, K. K., Chung, M. K., Krishnan, K., Kutyifa, V., . . . Lakkireddy, D. R. (2018). Cybersecurity for cardiac implantable electronic devices. *Journal of the American College of Cardiology, 71*(11), 1284-1288. doi:10.1016/j.jacc.2018.01.023

Henriksen, E., Burkow, T. M., Johnsen, E., & Vognild, L. K. (2013). Privacy and information security risks in a technology platform for home-based chronic disease rehabilitation and education. *BMC Medical Informatics and Decision Making, 13*(1). doi:10.1186/1472-6947-13-85

Kramer, D. B., & Fu, K. (2017). Cybersecurity concerns and medical devices. *Jama, 318*(21), 2077. doi:10.1001/jama.2017.15692

Ransford, B., Kramer, D. B., Kune, D. F., Medeiros, J. A., Yan, C., Xu, W., . . . Fu, K. (2017). Cybersecurity and medical devices: A practical guide for cardiac electrophysiologists. *Pacing and Clinical Electrophysiology, 40*(8), 913-917. doi:10.1111/pace.13102

Lechner, N. H. (2017). An Overview of Cybersecurity Regulations and Standards for Medical Device Software. *Proceedings of the Central European Conference on Information and Intelligent Systems,* 237-248.

Williams, P., & Woodward, A. (2015). Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. *Medical Devices: Evidence and Research,* 305. doi:10.2147/mder.s50048