IoT Devices in the Public Health Sector

Cayla Young
Old Dominion University

IoT Devices in the Public Health Sector

Cayla Young, Dr. Young Choi
CoVA CCI Undergraduate Research Program
Old Dominion University, Regent University

How might IoT devices and other advancements in technology raise privacy and security concerns for individuals within the public health sector?

Abstract

In this research, proper attention is drawn to privacy and security concerns with the integration of Internet of Things (IoT) devices in the public health sector. Often, not much attention is given to IoT devices and its vulnerabilities concerning the medical industry. Effects of COVID-19 contact tracing applications are explored through research of various source types. Mitigation techniques for these privacy and security issues is given. Focus is brought to topics outlining the risks associated with genetic testing companies and the vulnerabilities of data collection and data storage. Recommendations are provided to help consumers avoid these risks. Lastly, a comprehensive breakdown of two medical device technologies and how its vulnerabilities could severely harm patients is provided. Possible solutions and cybersecurity mitigation techniques are given to help manufacturers lessen risks for consumers and eliminate vulnerabilities for medical devices within the market. The discussion and research of this topic can bring awareness to the dangers of IoT devices in public health. This can help ensure the security and privacy of patients worldwide.

Introduction

The adaptation and advancement in technology has led to major shifts in modern society. Activities and processes that were once executed by hand or done in person are now either fulfilled online or done remotely. For instance, the use of smartphone devices has completely overturned its predecessor, the telephone, in daily activities. In business environments the telephone is still used frequently. However, outside of these workplace conditions, the smartphone still continues to be the popular choice. Even the addition of the telephone is testament to the adaptation of technology within modern society. Before that, messages and conversations were mostly conceived either in person or through mailing systems, utilizing mediums such as horseback travel, on foot travel, slaves, stagecoaches, steamboats, wagon trains, the Pony Express, and even balloons (Rickie Longfellow, 2017). Additionally, there has been an epic growth in the use of technology within contemporary global societies and economies. Conditions such as the Coronavirus's COVID-19 outbreak is living proof of this testament. The start of the pandemic from late December to early January honed in on the importance of a technologically based society. This novel pandemic led to the conversion of many institutions and businesses to online and remote formats. Primary schools, secondary schools, colleges, and major universities largely assumed an online presence requiring students, educators, and other colleagues to teach or learn from home. Throughout the nation, and globally, many video conferencing tools, namely Webex and Zoom, were used to achieve this newfound lifestyle. Companies and businesses that were able to convert to telework did so, and many employees were forced to work from home. Jobs and positions that were not able to successfully partake in the newfound domestic industry of teleworking were either furloughed or laid off completely, leaving many Americans jobless and unemployed.

Without the advancement of technology to its current prominence, the American economy, as well as economies in other parts of the world, would be in more of an economic crisis. The use of modern technology has been the redeeming characteristic for the American economy. With heavy social distancing and occupancy restrictions, the only businesses that kept the economy afloat, aside from essential businesses, were the remote and telework positions.

While the advancement and implementation of technology has benefited modern society by making everyday tasks easier, it has also propagated a sundry of disadvantages and drawbacks. From computers and cell phones to digital assistants, smart watches, smart TVs and other mobile and smart devices, they all present their risks, threats, and vulnerabilities. The connectivity of these devices to the Internet is often referred to as the Internet of Things (IOT). IOT devices are a network of instruments that connect to the internet such as personal items, home appliances, cloud services, and vehicles (Kim & Solomon, 2018). While this has provided many advantages to modern society like simplifying tasks, automating processes, and providing

better management, it has also created a risk for security and privacy concerns (BlueSpeed AV, 2016).

According to Security Today, in 2018 there were more than seven billion IOT devices connected and installed worldwide (Maayan, 2020). In 2019, that number jumped to over 25 billion devices (Maayan, 2020). In addition, marketing manager Kaylie Gyarmathy from vXchnge states that by the year 2027, there will be an estimated 41 billion IoT devices connected worldwide (Gyarmathy, 2020). This substantial amount of IoT devices are not the only parts of these statistics that will see a major increase globally. This adaptation of IoT technology, coupled with the numerous amounts of weak passwords, insecure networks, and lack of secure update mechanisms, will also contribute to the increase of risks, threats, and vulnerabilities that companies, businesses, and people will now be exposed to (Maayan, 2020). Users will face both privacy and security issues with the utilization of these devices. Some of the most frequent privacy and security issues that users may face are identity theft, security beaches, and the nescient collection of user data-which also creates entry points and leaves sensitive information vulnerable (Kim and Solomon, 2018; Insider Intelligence, 2020). Even with these common, generalized risks, threats, and vulnerabilities, these become even more problematic in the health industry. The exposure of sensitive data and the increased risk of security breaches is more detrimental when the lives of people are at risk. It is one issue for manufacturers and companies to gather data from a user's smart device without their knowledge and use that information to make calculated and planned decisions on the future success of the business; but it is an entirely different and more important issue when contact tracing applications are raising cybersecurity risks, genetic testing companies are creating vulnerabilities resulting in the lack of genetic privacy, and medical device manufacturers are ignoring high risks factors and deploying technology into the market. This is exactly what is happening now within the public health sector. The medical industry, especially since the COVID-19 pandemic, is now, more than ever, struggling to find the balance between using IoT devices to better hospitals and medical companies whilst maintaining security and privacy best practices and safety. Through this research, I will explore cases in which IoT devices posed significant threats to both the privacy and security of individuals and companies worldwide. Through the discussion of the novel Coronavirus's contact tracing apps, genetic testing companies using data for investigations, and the manufacturing of life-threatening medical devices, the problems that IoT devices can cause in the public health sector will be fully and extensively discussed so that proper attention to these issues can be given.

COVID-19 Contact Tracing Applications

With the recent outbreak of the novel coronavirus, COVID-19, countries around the world are trying multiple ways to slow down and stop the spread of the pandemic. With quarantine procedures, national lockdowns, and social distancing requirements, nations have

been in a desperate attempt to contain the virus. Consequently, certain countries and companies are developing contact tracing applications in their attempts to contain the virus. The top two mobile operating system competitors, Google and Apple, have designed an Exposure Notification API that enables a contact tracing feature on user's phones (Hall, 2020). Health authorities will be able to use this technology to create an Apple or Android app that will notify users if they have come in contact with someone who has recently tested positive for COVID-19. With user privacy and security as the basis for the API, Apple and Google are enabling the use of Bluetooth technology to alert users, via notifications, of when they have been in close contact with an infected person.

Recent software updates on both Android phones and iPhones will allow users to enable the feature on their device (Miller, 2020). Public health authorities in various countries and regions will be able to implement the Apple Google API into their COVID-19 app making it available to users within that region.

As for how it will operate, a beacon will be sent out via Bluetooth as a random Bluetooth identifier on the user's smartphone. When individuals come within a close proximity to each other, their devices will exchange the Bluetooth identifiers. Later, if one of these individuals test positive for COVID-19, they can voluntarily report their diagnosis to the Exposure Notification application within their region. More specifically and technically speaking, private special-purpose keys, called temporary exposure keys, will generate each day. That key will then generate random identification numbers called "rolling proximity identifiers" (RPIDs). With Bluetooth enabled, pings will be sent out once every five minutes. Every ten to twenty minutes, the RPID will change in order to reduce the risk of third-party trackers using the pings to track people's locations. The operating system saves each of the temporary keys and RPIDs it has come into contact with in the last two weeks (Cyphers & Gebhart, 2020). Because this app uses Bluetooth technology and regional data, it can help people in a community contain the spread of the virus. The app alerts users if they have been in contact with an infected person within the last fourteen days. This will allow individuals to self-quarantine, test if symptomatic, or avoid places they may have recently visited. The API itself does not constitute exposure. Instead, it includes a minimum of five minutes of interaction between individuals for it to be considered a match (Miller, 2020).

Editor and writer for 9to5Mac outlines an example of how the Apple Google Exposure Notification API might work:

> "Think of it like this: Person A and Person B spend more than 5 minutes together at a restaurant. During this time, their smartphones exchange the anonymous Bluetooth identifier. They go their separate ways, but Person A tests positive for COVID-19 a few days later and chooses to report that

> positive test via the Exposure Notification app. Person B will then receive a notification saying that someone they recently interacted with has tested positive for COVID-19.
>
> The public health authorities can determine what the next steps are. If ample testing is available, the app might suggest that Person B get tested even if they are asymptomatic. If testing is constrained, the app might suggest that Person B monitor for symptoms and only get tested if they become symptomatic, while also self-isolating."

This demonstration provides a clear and concise description on how the Apple Google API will work in a real-world scenario.

There have been numerous complaints from individuals, companies, and nations on the use of Google and Apple's Exposure Notification API. Many officials are concerned that the API's strict rules of prohibiting GPS location tracking, not sharing data with health officials, and not revealing where these person to person interactions occur is resulting in the technology being useless. Furthermore, when two people interact, it is not known where the contact took place. Even with the notification that a recently contacted individual has tested positive, that information is not relayed to contact tracing teams nor public health officials. Other officials within the public health industry also noted that contact tracing apps relying strictly on Bluetooth would face its own set of technical challenges. Many states and countries are asking for Apple and Google to relieve the API of some of its restrictions and give them more ability to collect user data. However, Google and Apple have informed authorities that allowing for more collection of data could lead to the increased exhaustion of battery life making consumers more agitated. Public health officials feel that the restrictions attached to Google and Apple's technology are contradictory to its purpose. Reed Albergotti and Drew Harwell, the authors of *The Washington Post* (2018), quoted Helen Nissenbaum, a professor of information science and director of the Digital Life Initiative at Cornell University, stating, "If it's between Google and Apple having the data, I would far prefer my physician and the public health authorities to have the data about my health status. At least they're constrained by laws," (p. 2). Many are suggesting that the contact tracing system is not at all contact tracing. Moreover, many officials feel that there is an unbalance between the importance of privacy and the importance of public health and its potential to save lives. This discrepancy between tech giants and local health officials is causing many to believe that the bigger, more important global health issue is being overlooked.

Because of these disagreements, some companies and developers have taken to creating their own COVID-19 contact tracing apps without the use of Apple and Google's technology. For example, North Dakota developers have created their own COVID-19 app called Care19 (Albergotti & Harwell, 2020). This collects and uses location data as a memory tool. It would also allow public health workers to contact the individual upon testing positive for Coronavirus to further collect and review data over the previous two weeks. This could assist health workers in finding out what locations the individual may have recently visited. Nevertheless, Apple and Google's lack of restriction removal has forced developers to start from scratch in creating their own applications without their technology. In the case of North Dakota, developers were forced to create two separate apps: one for contact-tracing teams and one using the Apple-Google system. This, however, creates the fear that less of the population might adopt these apps, creating greater confusion and longer delays for data that could potentially save lives (Albergotti & Harwell, 2020).

Another example of developers trying to create their own contact tracing apps is a case in Alberta, Canada. A contact tracing app was built, but again faced restrictions with iPhones due to its limitations set on Bluetooth capabilities.

Some have argued against companies' and developers' disdain towards the lack of data collection with Apple and Google's technology stating it is better to just adopt the API and all its restrictions as it will be better than what the government could develop (Albergotti & Harwell, 2020, p. 3). Likewise, companies are adding that limiting the information that these apps can collect with use of the Apple-Google technology is actually a good thing because it can raise the adoption rate within the population if people know that their location is not being gathered and saved. On the contrary, a poll conducted by the Washington Post-University of Maryland Poll, found that Americans trusted the collection of their location and information more with public health agencies than Apple and Google. Ashkan Soltani, a former chief technologist of the Federal Trade, Commission stated he would be more comfortable with health agencies collecting data than Apple and Google as they would have legal protections and a dedicated operational security team (Albergotti & Harwell, 2020).

Germany, Italy, and the Netherlands have already indicated that they will use Apple and Google's API. Other countries, such as Norway and the United Kingdom, however, are creating their own apps which will take the different approach of a centralized system lacking the restrictions and constraints that the Apple-Google system possesses.

However, many of them are facing functionality issues. For instance, in an attempt to avoid battery consumption and privacy problems, Apple devices, as mentioned previously, disallows app makers ability to utilize Bluetooth tracking in the background. This would mean that users would be forced to keep the app open and running at all times to ensure its functionalities are being used. Some developers have asked Apple and Google for help concerning its functionality issues but were prompted to use the Apple-Google system instead. Moreover, compliance would nullify the recording of user location data and the distribution of information to contact tracing teams leaving developers in the exact same dilemma (Albergotti & Harwell, 2020).

In an attempt to relieve users of potential privacy and security concerns, Google and Apple are strictly using Bluetooth technology with no use of location data. Their main goal is to collect as little information and data as possible to avoid not only privacy concerns for individual users but also security concerns from potential hackers. Because of this, Apple and Google have strict privacy requirements that health authorities must adhere to with use of their API. For instance, with the adoption of their API, these applications must remove all Location Services features whilst also adopting the privacy frameworks of the Google Apple API. Many health officials and app developers see this as an issue because they rely on location data to map out what areas contain higher infection rates compared to others. Without this information, health officials have no way of telling what locations and regions have more at-risk potential. Google and Apple have also noted that ordinary developers cannot access this API, only public health authorities are able to use this API for the purpose of COVID-19 (Miller, 2020).

Since the development of the Exposure Notification API, more security features have been implemented. For instance, all metadata associated with Bluetooth is encrypted. This will make it harder to discover and identify an individual user. Additionally, according to Chance Miller (2020), “Temporary Exposure Keys are now generated randomly instead of being derived from a tracing key,” (pg. 1). It is also important to note that these keys are only stored for a maximum of fourteen days locally on the user’s phone.

Despite the privacy and security concerns that people are expressing, Apple and Google are making strides to keep users safe such as making the API voluntary (meaning users must opt in to use the system) and storing and processing contact tracing data only on the user’s device.

Nonetheless, experts are voicing their concerns with the new SwissCovid app that uses the Apple-Google API. Experts giving their insight on the new Switzerland app are concerned that without a centralized organization supervising the alerts to ensure that at-

risk users are being warned, there is a chance that the app will receive an influx of false positives. Additionally, other experts around the world have also suggested that the use of a proximity tracking system, such as the Apple-Google API, could lead to the discovery of infected persons. In one example, if an individual recently interacted with a friend, the individual might be able to later figure out that the person is infected by comparing their own contact log to recently visited persons (Cyphers & Gebhart, 2020). Further, the RPIDs that are generated from the temporary exposure keys could be used by bad actors to connect them to identities using facial recognition and other advanced technology. This would allow the potential for the creation of a database of infected persons.

Another issue that may occur with the use of proximity tracking apps is its vulnerability concerning the once-per-day diagnosis keys. These diagnosis keys are the uploaded versions of the user's temporary exposure keys after confirmation that the individual has been infected. A hacker could gather the RPIDs from various locations through static Bluetooth beacons in public areas or by convincing thousands of users to install an app. From here, a linkage attack could occur once the user has uploaded their daily diagnosis key to the public registry. In a single day, the hacker could link all of that person’s RPIDs collectively. This can expose the user’s daily routine such as where they live, work, or spend their time (perhaps sensitive locations such as churches and medical offices). Because of its uniqueness, a person can be identified simply by his or her daily routine.

As explained by Bennett Cyphers, Staff Technologist, and Gennie Gebhart, Associate Director of Research both at Electronic Frontier Foundation (2020), one possible mitigation to an attack such as the one explained above, might be shortening the time from daily keys to hourly keys. This means that a single diagnosis key used to generate RPIDs will be shortened but at the cost of increasing the download size of the exposure database (Cyphers & Gebhart, 2020).

Another possible vulnerability that could lead to the identification of a person is through the data created by the proximity app. Because each person’s phone logs data of their physical proximity to other devices, a person with access to the proximity app data can see the contact information logged. The data and information in proximity may also be gathered by police if requested. A possible solution for this issue is with the use of encryption and passwords. Users should also be provided the ability to turn off the app and delete proximity data from certain periods of time.

There are a few other possible vulnerabilities that are created with the use of these contact tracing apps. Because there is no way to verify that the Bluetooth identifier sent from a device actually came from that device, hackers could collect identifiers (using Bluetooth beacons) from several devices and rebroadcast them out into a busy area. Users in the area would

log the identification numbers potentially creating many false positive cases. This would devalue the trust in proximity tracing apps and possibly the public health system entirely (Cyphers & Gebhart, 2020). Some are also worried that people could falsely claim to have COVID-19 since there is no authentic way to verify that. It was suggested that Google and Apple may be able to use health agencies to verify that a person has actually been infected before uploading their diagnosis (Robertson, 2020).

Genetic Testing Companies

Genetic privacy is an important factor in maintaining the confidentiality of every single individual because it will not only keep the person from losing large amounts of money but also help retain one's privacy and security from the potential exploitation of third-party companies and/or other undesirable parties. This is demonstrated in the case of Henrietta Lacks, an African American woman whose cells were covertly stolen during biopsy treatments for cervical cancer (Truog, Kesselheim, and Joffe, 2012). In this case, Lacks's diagnosis of cervical cancer led to radium treatments. Biopsies were done on Mrs. Lacks by the cancer and virus researcher at the Johns Hopkins Hospital, Dr. George Otto Gey, who, without her permission, took healthy and cancerous tissues from her cervix. It was soon discovered that her cells were unique in that they doubled every 20 to 24 hours allowing for medical laboratory experiments to be performed due to their ability to live long enough for the experiments to be conducted. This medical breakthrough was important as Lacks's "HeLa" cells have have since been used to test the effects of radiation and poisons as well as testing the "effects of toxins, drugs, hormones, and viruses, on the growth of cancer cells" (Butanis, 2017). Her cells aided in the development of vaccines such as the polio vaccine. They have also been used to study the human genome and develop further research on the study of how viruses work (Butanis, 2017).

This complete and total lack of genetic privacy resulted in a patients' DNA being collected and used without permission. Henrietta Lack's story brings attention to another important topic regarding genetic privacy in the public health sector in regards to the advancement of technology through the use of IoT devices.

In keeping genetic information private, there is a lesser chance of private information being hacked/stolen or even being posted online for the general public to see. This statement is particularly true in the case of the Personal Genome Project, or PGP. Started in 2015, according to Xinghua Shi and Xintao Wu, doctors and authors for the New York Academy of Sciences, PGP, based at Harvard Medical School, is an open archive of human genomes where participants volunteer to share their DNA for medical research (Shi & Wu, 2017). In accordance with George J. Annas (2014), a Chairman and Professor of Health Law, and Sherman Elias, a geneticist and former chair of Obstetrics and Gynecology at Northwestern University's Feinberg School of Medicine, although good-sounding, participants, whose identities were kept private, were

allowed to "upload 23andMe, a genetic testing company, genotyping files to public profile webpages" (Shi & Wu, 2017; Annas, 2014, p. 1). Because participants used the default name convention, their full first and last names were disclosed. This has since been fixed because PGP changed their file naming system. Although corrected, this simple error presents the idea of potential security risks that come along with the continued use of genetic scientific research especially and particularly when genomic information is collected from multiple data sources. Shi and Wu stated that even in projects where de-identified genetic data is collected from anonymous users, people are still able to exploit and trace the identity of unknown genomes. They can pinpoint the source of the data by using birthdays, gender, and 5-digit zip codes. According to them [Shi and Wu], thirty percent of PGP participants were identified by the use of demographic profiles (such as birthdays and zip codes). These anonymous-access beacons can be exploited, and genomic sharers can be reidentified encroaching genetic privacy (Shi & Wu, 2017). If exploiters are able to use birthdays and zip codes to identify the physical makeup of someone's being, one must then consider the importance of genetic privacy and security, especially in a society that continues to adopt technology within the public health sector.

In the article titled "Why a DNA data breach is much worse than a credit card leak," Angela Chen, a science reporter for The Verge (2018), states "Genetic testing sites are treasure troves of sensitive information." In 2017, MyHeritage, which Chris Phillips, a member of the Forensic Genetics Unit at the Institute of Forensic Sciences, defines as another online genetic testing vendor, revealed that hackers breached over 92 million of its accounts (2018). Chen said that they never accessed genetic data, but instead the emails and passwords. However, with the increasing amount of popularity of these online genetic testing websites and technology, who is to say this will not happen (Chen, 2018)? Given the increasing rate of the advancement of technology to the point where someone's DNA can be identified by their birthday and zip code, it is critical to consider that having information as sensitive as the physical map of one's entire body online is not safe. Once again, genetic privacy and its specific relation to technology, the internet, and IoT devices must be taken into account.

There are even more situations where this topic becomes a problem. For example, law enforcement and investigators have even furtively solved crimes using these genealogy websites without the permission of the DNA owners. And while this sounds like a progression within law enforcement, it is actually quite the opposite. Avi Selk, a reporter for *The Washington Post*, reported that James DeAngelo, the "Golden State Killer" (as he is commonly known by) who is responsible for 13 murders and more than 50 plus rapes and over 100 burglaries, became a trending topic in the late 70s and 80s (Selk, 2018). Based upon DNA samples collected by law enforcement, it was proven that James DeAngelo was indeed the serial killer that terrorized a number of victims in California during that time.

The culprit responsible for this discovery was GEDmatch. Rachel Becker, another science reporter for The Verge, says that GEDmatch is another genealogy website that allows users to connect with past and current relatives by sharing their full genetic information (Becker, 2018). Because this website is entirely open to the public, there were no hurdles or obstacles for the investigators to track him down. It is said in this article that the investigative team was able to create a fake profile to track down the serial killer using DNA collected from a murder that he committed 37 years prior. Working with genealogists, the investigators were able to match his DNA to that of some of his relatives. James DeAngelo had lived in areas relative to the locations that the Golden State Killer's crimes took place. The investigators were then able to make a match when DNA from something DeAngelo had thrown away was the same to the DNA that was collected at the murder scene. Becker (2018) writes, through various statements from GEDMatch, that the company was not aware of the investigation. GEDMatch also stated "Although we were not approached by law enforcement or anyone else about this case or about the DNA, it has always been GEDmatch's policy to inform users that the database could be used for other uses, as set forth in the Site Policy," (p. 2). They also proceeded to mention that although GEDMatch is used for genealogical research, they want their users to be aware that their DNA may be used for identification purposes such as identifying "relatives that have committed crimes or were victims of crimes," (Becker, 2018, p. 2). This again shows the risks of putting personal DNA on genealogy websites and other places online. If one does not carefully read the terms and conditions agreements and website policies, it can then become easy to fall victim to cases like these. The controversy especially arises in cases where law enforcement solves crimes by the use of DNA collected through their own databases (Becker, 2018). For instance, the FBI's national genetic database consists of DNA from federal convicts and arrestees who have yet to be convicted. This practice can be controversial because it exposes citizens to further scrutiny because a relative of theirs is in the DNA database (Becker, 2018). This can be a violation of their civil rights (Becker, 2018).

Furthermore, in the words of Chris Phillips (2018) "Genealogists have identified missing persons with increasing precision, as…those wishing to discover their distant relatives using the proprietary company databases and GEDmatch," (p. 186). This simple fact means that genetic privacy can be further exploited due to the advancement of technology. This is not ethical because one's privacy is being removed. It can also lead to potential cybersecurity breaches and future hacks, just like when the MyHeritage security breach occurred. The use of IoT devices and the internet has created the risk and vulnerability for these genealogy websites and its databases. Without the proper legal protections and technical solutions, these databases promote the risk for cybersecurity breaches of improper data collection and misusage. Considering the importance and value that one's physical makeup possesses; its risks of exploitation can become threatening. Once more, these exploitations within IoT devices can encourage hackers to utilize them for financial and personal gain.

Medical Devices

The combination of medical devices and technology helps simplify the lives of those with certain health conditions and complications. An example of one company that utilizes technology to aid those who face such complications is Medtronic. Medtronic is a leading manufacturer of medical devices first getting its initial start in the creation of portable pacemakers by founder Earl Bakken (Roehr, 2018). While these medical devices have been used to take on some of healthcare's greatest medical challenges that patient's face, there are quite a few vulnerabilities that researchers have discovered within their technology. If exploited by bad actors, some of these devices' vulnerabilities can be life threatening to the consumer.

In one case, researchers Billy Rios and Jonathan Butts of QED Secure Solutions discovered a hack that allows hackers to control pacemakers remotely, giving them the ability to deliver or withhold shocks to a patient's pacemaker (Newman, 2018). This creates harm for the patient in that they may receive shocks that they don't need or be denied shocks that they do need, both potentially creating life threatening circumstances.

The researchers coordinated their own experiment using Medtronic equipment obtained from third party resellers and medical supply distributors and demonstrated their findings at the Black Hat security conference in 2018. They showed how the company's pacemaker programmers could be hacked to install malicious updates through Medtronic's software delivery network taking advantage of Medtronic's lack of digital code signing. It should be mentioned that the pacemaker programmers use Medtronic's software delivery network to bring updates to the equipment so that healthcare professionals may tune the implanted pacemakers. The compromising of these pacemaker programmers enabled the researchers to access the implanted pacemakers themselves through the bugs in the company's software delivery network.

The researchers noted that a mitigation for this vulnerability is through the use of digital code signing. They also noted that this digital code signing would allow the company to ensure and cryptographically verify that the software and any applications used have not been tampered with. They even mentioned that other competitor companies running their software on the same operating systems (WindowsXP) have already implemented code signing, lessening their risks of attacks. The act of running such software on WindowsXP poses its own vulnerabilities given that WindowsXP has stopped receiving support from Microsoft since April 8 of 2014 (Microsoft, n.d.). Further, Butts and Rios conclusively added that these serious matters should not be downplayed by Medtronic as they could promote the risk for serious attacks. A quote from Jonathan Butts was expressed stating, "We were talking about bringing a live pig because we have an app where you could kill it from your iPhone remotely and that would really demonstrate these major implications. We obviously decided against it, but it's just a mass scale concern. Almost anybody with the implantable device in them is subject to the potential

implications of exploitation," (Newman, 2018, p. 4). In addition to the above vulnerabilities, these pacemakers also possess another vulnerability: researchers from the Medical Device Security Center revealed that many of these pacemakers contain unencrypted radio signals. These radio signals allow the pacemakers to be reprogrammed (Sorrel, 2008). Although the kit may be expensive, and attacks must be in close proximity, the possibility of such an attack is real. With the right kit and the absence of security, hackers can utilize this exposure to acquire control of the pacemaker and enact attacks possibly causing ventricular fibrillation or cardiac arrest.

Researchers Butts and Rios also suspected, through the use of their proof of concept, the lack of authentication and integrity checks. However, since there was no way to validate this suspicion on their proprietary cloud infrastructure, they created their own proof of concept by developing a replica of the environment and conducting experiments on it.

Medtronic did take heed to some of the advice that the researchers provided following their experiments and security research, such as resolving a cloud vulnerability that could allow hackers remote access to alter pacemaker data pertaining to a patient. However, the company was hesitant to make any security changes to their medical equipment and network, if any, despite the researchers' discoveries. In some instances, they even denied the findings stating they "revealed no new potential safety risks" (Newman, 2018, p. 3). Despite the researchers' and company's disagreements, the Food and Drug Administration (FDA), who often gets involved in matters regarding Medtronic's security concerns, stated they value the work of researchers, industry, academic, and the medical community in matters that concern the health and safety of consumers and patients. In fact, especially in matters regarding cybersecurity, they implied that they encourage it. Consequently, the FDA created the Medical Device Safety Action Plan which seeks device regulation in an attempt to improve medical device safety for the healthcare needs of patients (Center for Devices and Radiological Health of the FDA [CDRH], 2019; Bryant, 2018). Further, they proposed a new plan that will establish the CyberMed Safety (Expert) Analysis Board (CYMSAB). The CYMSAB would bolster their cybersecurity efforts to improve their medical device safety plan by pushing "integration of patient safety and clinical environment factors into assessments and validations of high-risk devices and incidents," (Eisenhart, 2018; Dodson, 2019).

Medtronic has undergone another security vulnerability regarding its medical technology. Its insulin pumps provide both solutions and complications for many of its consumers. Using similar methods as investigated with the pacemaker, Butts and Rios were able to demonstrate the process a hacker could use to remotely connect and control a Medtronic, radio enabled insulin pump (Newman, 2019). Even further, the development of an Android app was enough to take control of a pump and either deliver or deny insulin injections. These MiniMed pumps, as they are referred to, contain buttons that allow patients to deliver insulin injections also known as

boluses. An attribute of the medical device is its ability to be remote controlled. MiniMed insulin pumps come with remote controls that give caregivers and other medical professionals the ability to control the pumps from a short distance. These remote controls, which resemble car key fobs, communicate with the MiniMed pumps via radio signals. According to Rios and Butts, it is not hard to determine the frequency at which these two devices communicate. Addedly, these radio signals are unencrypted. Researchers Jesse Young and Carl Schuett, also working along Rios and Butts, found that with reverse engineering techniques, the two methods of simple encoding and validity checks, both used to protect the signal, could be easily compromised. The bad actor would then be able to capture the remote control's commands. This would enable the attacker to utilize open source software to program a separate radio. This second radio could then be disguised as an actual MiniMed pump controller. The pump, not realizing the fraud controller, would trust and execute any commands sent from it. This decoy could then be controlled through a smartphone app to launch attacks and execute commands. This process is similar to that of universal remote apps on smartphones that are used to control televisions. In this example, with access to the smartphone app, the attacker could distribute unnecessary insulin injections or override essential injections that the patient is trying to give themselves.

To attack a specific insulin pump, the perpetrator would need to know the serial number of the device. If using a brute force type of technique, a hacker would be able to run through every possible string of numbers to identify the specific serial number of the target device. That is what researchers Butts and Rios did in their investigation. They added a functionality to their remote that allowed them to conduct the operation. The only other stipulation that an attacker would be required to adhere to is the limited range of the remote. The individual would need to be in a close enough range for the remote to control the MiniMed pump. However, Butts and Rios mentioned that signal-boosting equipment could be used to expand the radius that the remote can operate in, helping to alleviate this issue.

Despite the severity of these vulnerabilities, Medtronic has been languorous in their attempts to make any security changes. Although the FDA, the Department of Homeland Security, and Medtronic warned users of its security problems, an adequate solution has yet to be provided. An inapt solution was given to turn off the remote access of the insulin devices, but that suggestion was quickly rescinded. It was determined that the importance of enabling caregivers the ability to dispense injections remotely outweighed that of completely removing the function. Furthermore, not all patients will remember to disable the feature nor would all of them know of the security issue regardless.

The insufficient knowledge and methods to patch the devices' flaws led to the eventual recall of the devices on behalf of the risk assessment and analysis by Medtronic and the findings of researchers observed by the FDA. This voluntary recall, as it has been named, promotes users to return and cease use of the 4,000 plus insulin pump models with this vulnerability. In some

countries, programs will allow consumers to exchange these old devices for newer models. In a statement released by the company, it has known of the vulnerabilities in the MiniMed pumps for years. After 2011, however, the company began to implement security features into its newer models. Medtronic insists that these newer models are able to "communicate in completely different ways," (Newman, 2019, p. 8). They also noted that since these upgrades, many current users are not being affected by this cybersecurity dilemma. With most of the impacted users residing outside of the United States, the voluntary recall was a slow process because communicating with regulatory agencies to issue international voluntary recalls was challenging. The FDA and Medtronic were careful to not use the word "recall" and instead considered it more of a "safety notification." This distinction is imperative in that it ensures no instance of a ban or outlaw can occur. The FDA wants to ensure that users who are in need of these older pump models are not afflicted despite its shortcomings. These distinct users are a part of a specific group of MiniMed patrons that need older models in order to "loop." Thus, loopers require older versions of the MiniMed pumps for its ability to be hacked. When older pump models are used in conjunction with glucose monitors, the two devices can communicate with each other creating a feedback loop. The devices can then be programmed to automatically calculate and deliver sufficient insulin injections to a patient. This feedback loop mechanism operates as a sort of artificial human pancreas.

Of the 4,000 people that are currently being impacted, the users who may want to upgrade to newer models have the option of doing so for free. With the FDA acting as a liaison between researchers and Medtronic on the universal remote-like hack on MiniMed Pumps, they, again, encourage and desire the collaboration efforts between medical device manufacturers and researchers. The cooperation between researchers and companies can speed efforts in ensuring vulnerabilities are accurately and quickly identified upon or before entering the market. In the instance where use of these technological devices in the healthcare industry becomes life threatening, proper action should be taken to mitigate or completely eradicate risks.

Solutions

With the integration of these devices in the medical industry, companies, consumers, experts, and researchers must take into consideration the increased risk that such devices hold. Therefore, appropriate mitigation techniques and necessary cybersecurity best practices are needed. While this section will be labeled solutions, these are mere recommendations for the respective parties to consider or implement subsequent to the rapid adoption of modern technology.

In regards to the recent production of contact tracing apps to help slow the spread of COVID-19, many procedures and methods can be used to further secure the technology. Bennett Cyphers and Gennie Gebhart of the Electronic Frontier Foundation, (2020) outlines ways that

app developers and Apple and Google can take action. These will be stated and explained further on.

Apple and Google have informed the public about its intent to have public health authorities be the main developers of these contact tracing apps using its API technology. Unfortunately, many health agencies lack both the resources, technology, and knowledge to develop such apps and will most likely seek private companies to carry out its requests. It is important that these private companies follow the same privacy and security accommodations that Apple and Google have set forth. Consequently, they will have much responsibility in ensuring this is correctly executed.

The first step developers can take in compliance with Google and Apple's guidelines is to maintain the decentralized approach for storing and sharing data. Keeping data temporarily stored locally, on the user's device, will help in this approach. Furthermore, Cyphers and Gebhart advise developers against sharing data over the Internet that goes beyond the diagnosis keys users upload when they become infected. Moreover, analytics libraries that share data to third party companies should be avoided as that will put users at risk and void trust. Technical safeguards and policy safeguards can ensure that data is used strictly for COVID-19 reasons. It is also highly advised that developers, along with Apple and Google, are forthright with their intentions in relation to data collection as well as provide ways to stop the collection of data. In addition, users should be given the ability to start and stop the sharing of RPIDs coupled with the ability to see a "list of the RPIDs they've received, and delete some or all of that contact history," associated with it (Cyphers & Gebhart, 2020, p. 8).

In addition to being forthright with regards to data collection, they should also be straightforward with the total workings of its app and the risks stemming from it. Source code and documentation should be published so that tech savvy users may be able to further analyze the technology and make sure it is performing and doing only what is expected in turn establishing better trust between the user and developer. Security audits and penetration testing will help to harden this technology as well.

Cyphers and Gebhart include that while the health crisis is underway, developers should avoid adding nonessential and unnecessary features while also avoiding advertisements as they have the potential to exploit user data and cause other technical complications. Account sign up should be discouraged and equally avoided. Health authorities and developers should steer clear of rushing the creation of the technology so that adequate care and attention is given to possible vulnerabilities with proper testing being conducted before release. Wherefore, users may need to exercise caution with newly released apps utilizing Apple and Google's technology.

Because Apple and Google are providing the base technology for developers and public health authorities to use, they should adhere to certain precautions. They should be flexible with their technology by communicating with app developers to provide users the ability to allow them to delete parts of their contact log including any data collected from that device. Another way this flexibility may be exercised is by creating easy opting in and opting out methods for user discretion. This will give people the option to rid themselves of the voluntary API proximity tracking technology since it has been recently integrated into both Android and iOS operating systems. As with app developers, they should also open source their technology for the tech savvy individuals and security analysts.

To establish trust, Apple and Google could prohibit proximity tracking apps from accessing device identifiers such as mobile ad IDs. Apple and Google can make sure the contact tracing apps comply with privacy requirements and methods used to protect user data.

Enhancing control of what app developers can access, more trust can be established between Google and Apple and its customers. Although both companies promise that the API can only be used by public health authorities, there are still cybersecurity measures that need to be implemented and exercised. Being transparent with consumers along with making sure they are not favoring and excluding certain governments and companies from their restrictions and guidelines will help to keep the public's trust and confidence in both the companies. Conclusively, when the Coronavirus crisis is over, Google and Apple should publicly establish clear guidelines detailing and defining the end of the crisis so that the technology can be properly terminated, without being repurposed for other things like tracking seasonal outbreaks or finding crime witnesses, when everything is over and done. Utilization of public health authorities to clearly define the end of the crisis and the removal of the API is recommended (Cyphers & Gebhart, 2020).

User security and privacy should be of top priority to companies like Google and Apple in order to receive support for their API and the apps created following it. Privacy risks should be kept to a minimum and consent should be required from end users before use. These examples and recommendations will help to mitigate risks associated with the integration of IoT devices and technologies coinciding with them.

Privacy and security safeguards can be taken by both the consumer and company in relation to genetic privacy. For concerns regarding DNA privacy, it is up to the consumer to understand the risks associated with genetic testing companies. Users must increase their knowledge in order to prevent falling victim to the attacks that can be experienced with usage of these companies. Reading the terms and conditions and end user agreements will help the consumer to make a determination of the utilization of these tools. DNA testing companies that are not well known should be avoided. This will give users more potency if anything goes wrong

because well-known organizations such as Ancestry.com have a bigger platform and may be easier to contact employees in the event that an incident occurs. Also, they are typically held more accountable than smaller companies. Often, their privacy policies are more thorough and extensive (Ravenscraft, 2019). If prompted by companies to use data for other reasons outside of providing DNA results, such as for research, this should be denied. If already accepted, a user may be able to revoke this permission. However, if the third-party company has already received user data, it may be impossible to have this data deleted or removed (Ravenscraft, 2019). Utilizing proper healthcare agencies will be the safest and most secure way of accessing genetic information as DNA testing companies often have a low baseline for protection.

Additionally, companies can take action by being fully transparent with its customers. Not only is this important, but they must make this information easily and readily available. Law enforcement should also step in to help further protect consumers.

Users who fail to use the above techniques or establish confidence in such companies should avoid them altogether. Ultimately, the best way for users to avoid these risks, will be to read the company's privacy policies. This will detail information such as what type of data the company collects as well as how it uses that data (Ravenscraft, 2019).

Lastly, there are protective measures medical device manufacturers can use and procedures they can undergo to achieve safer standards for patients. Consistent testing before release of a product can aid in this objective. Often, researchers conduct numerous investigations on manufacturer's technology and find errors that would have been discovered with proper examination and testing beforehand. More importantly, companies such as Medtronic must take the corrective measures once vulnerabilities and flaws within technology are discovered. This will prevent potential cybersecurity breaches and technical aberrations that may come further in time. With that, Dan Dodson (Dodson, 2019) of Fortified Health Security outlines extra safety precautions and measures that providers and manufacturers can take to better cybersecurity health.

With the FDA's Medical Device Safety Plan, a sufficient guideline can be used to help exercise these measures. According to Dodson, the plan will seek to lessen risk and prevent security breaches. This includes "considering a requirement for firms to update and patch device security in product design and submit a 'Software Bill of Materials' to the FDA, updating pre-market guidance on medical device cybersecurity, considering a new postmarket authority to require firms to adopt policies and procedures for coordinated disclosure of vulnerability, and exploring the development of a CyberMed Safety (Expert) Analysis Board," (Dodson, 2019). In addition to these methods, further recommendations from Dodson are discussed onward.

Manufacturers should be responsible for the testing of each product before distribution to medical device providers. If an update needs to be delivered to devices, providers must have confirmation that the update has been tested and vetted by device manufacturers for performance issues. An efficient way of doing that is by requiring manufacturers to submit a service level agreement within a given time frame that will pertain to device vulnerabilities prior to distribution (Dodson, 2019). Manufacturers should also be prompted to submit threat intelligence and vulnerability reports to respective agencies so that providers may be aware of security risks and adapt accordingly.

Dodson mentions that providers and manufacturers need a streamlined form of communication. By setting standards for how manufacturers may communicate with providers, vulnerabilities and device issues can be addressed and resolved in a timely manner. The method of communication coupled with the frequency of communication will be effective in solving this issue and will lead to better security for devices.

Hardening of the device before it enters the market will lessen the steps needed to deploy security updates and testing procedures once the device reaches the market. To do this, the FDA can require manufacturers to indurate their devices to a known security standard before the full release.

According to Dodson, device connectivity requirements should be properly evaluated. Providing end users with a clear connectivity path will help monitor malicious activity when using certain widely used technologies. A clear connectivity path will facilitate how and what devices should communicate with the technology and what communication types are normal. This will give users a better understanding of how certain devices will perform on the network and also help them differentiate between what is normal device performance and behavior and what is not. Full-time connected devices on the network could be monitored using performance monitoring techniques provided by the manufacturer helping to create a long-term strategy for these devices.

The aforementioned measures and techniques should be practiced for the health and safety of consumer patients. Cybersecurity should be taken seriously as well as the methods used to ensure it. It is the responsibility of both manufacturers and providers to aid in these devices being properly secured and tested before release into the market. Thus, a consideration for the amount of resource consumption is conspicuous. A cogitation for the large quantity of resources such as the amount of bandwidth needed to support the vast amount of newly accumulated data to exercise these introduced techniques is necessary. Providers and manufacturers can provide solutions or replacements for high risk devices. With the growing number of cyber-attacks in the world today, especially with the onset of the pandemic, it is pivotal that these issues are given priority from its respective parties for the security, privacy, and safety of patients.

Conclusion

With the ever-expanding use of technology, the prominence of cyber-attacks is in direct correlation to this increase. Researchers, manufacturers, tech corporations, genetic testing companies, and engineers will need to find new and innovative solutions to enhance the security of IoT devices to ensure the safety and security and the preservation of privacy for individuals. Following the preceding examples, these entities will have a greater chance of solving the issue at hand. As more of the population adopts technology, the need for creative solutions regarding cybersecurity will also be of greater necessity. The previous cybersecurity enhancing proposals are not answers to these concerns but instead possible suggestions that may later become solutions. However, it is up to the appropriate parties to take action in protecting end users. More importantly, the involvement of the Internet of Things devices becomes more significant within the public health sector due to its heightened, life-threatening potential. As humans become more reliant on technology in the medical industry, privacy and security will need to be prioritized substantially.

References

Albergotti, R., & Harwell, D. (2020, May 15). *Apple and Google are building a virus-tracking system. Health officials say it will be practically useless*. The Washington Post. https://www.washingtonpost.com/technology/2020/05/15/app-apple-google-virus/

Annas, G. J. & S. Elias. (2014). 23andMe and the FDA. *The New England Journal of Medicine, 370* (11) 985–988. https://odu-primo.hosted.exlibrisgroup.com/permalink/f/1ucqpjv/TN_proquest1507794875

Becker, R. (2018, April 26). *Golden State Killer Suspect Was Tracked down through Genealogy Website GEDmatch*. The Verge. www.theverge.com/2018/4/26/17288532/golden-state-killer-east-area-rapist-genealogy-websites-dna-genetic-investigation

Bryant, M. (2018, July 23). *5 key parts of the FDA Medical Device Safety Action Plan*. MedTech Dive. https://www.medtechdive.com/news/5-key-parts-of-the-fda-medical-device-safety-action-plan/528210/

Butanis, B. (2017, April 12). *The legacy of Henrietta Lacks*. Johns Hopkins Medicine. www.hopkinsmedicine.org/henriettalacks/index.html

Center for Devices and Radiological Health of the FDA. (2019, September 18). *Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health*. Food and Drug Administration. https://www.fda.gov/about-fda/cdrh-reports/medical-device-safety-action-plan-protecting-patients-promoting-public-health

Chen, A. (2018, June 6). *Why a DNA Data Breach Is Much Worse than a Credit Card Leak.* The Verge. www.theverge.com/2018/6/6/17435166/myheritage-dna-breach-genetic-privacy-bioethics

Cyphers, B., & Gebhart, G. (2020, April 28). *Apple and Google's COVID-19 Exposure Notification API: Questions and Answers.* Electronic Frontier Foundation. https://www.eff.org/deeplinks/2020/04/apple-and-googles-covid-19-exposure-notification-api-questions-and-answers

Cyphers, B., & Gebhart, G. (2020, April 28). *Apple and Google's COVID-19 Exposure Notification API: Questions and Answers*. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2020/04/apple-and-googles-covid-19-exposure-notification-api-questions-and-answers

Dodson, D. (2019, September 19). *FDA Medical Device Safety Action Plan: Will it Work?*. Fortified Health Security. https://www.fortifiedhealthsecurity.com/blog/fda-medical-device-action-plan-work/

Eisenhart, S. (2018, April 27). *US Regulators Propose Expanded Medical Device Cybersecurity Approach*. Emergo. https://www.emergobyul.com/blog/2018/04/us-regulators-propose-expanded-medical-device-cybersecurity-approach

Gyarmathy, K. (2020, March 26). *Comprehensive Guide to IoT Statistics You Need to Know in 2020*. vXchnge. https://www.vxchnge.com/blog/iot-statistics

Hall, Z. (2020, July 13). *Which U.S. states are using Apple's exposure notification API for COVID-19 contact tracing?* 9 to 5 Mac. https://9to5mac.com/2020/07/13/covid-19-exposure-notification-api-states/

Kim, D., & Solomon, M. G. (2018). *Fundamentals of information systems security* [pdf]. Jones and Bartlett. https://drive.google.com/file/d/1B_I3GJ3Fp4jmvvt5qe9igOtjdb9TGVED/view?usp=sharing

Longfellow, R. (2017, June 27). *Back in Time: Transportation in America's Postal System.* Federal Highway Administration. https://www.fhwa.dot.gov/infrastructure/back0304.cfm

Maayan, G. D. (2020, January 13). *The IoT Rundown For 2020: Stats, Risks, and Solutions.* Security Today. https://securitytoday.com/articles/2020/01/13/the-iot-rundown-for-2020.aspx#:~:text=How%20many%20IoT%20devices%20are,IoT%20devices%20reached%2026.66%20billion

Microsoft. (n.d.). *Support for Windows XP ended. Microsoft.* https://www.microsoft.com/en-us/microsoft-365/windows/end-of-windows-xp-support#:~:text=Support%20for%20Windows%20XP%20ended,to%20a%20modern%20operating%20system.

Miller, C. (2020, June 19). *Here's how Apple and Google's exposure notification API works while securing privacy*. 9 to 5 Mac. https://9to5mac.com/2020/06/19/apple-and-google-exposure-notification-api/

Newman, L. H. (2018, August 9). *A New Pacemaker Hack Puts Malware Directly on the Device*. https://www.wired.com/story/pacemaker-hack-malware-black-hat/

Newman, L. H. (2019, July 16). *These Hackers Made an App That Kills to Prove a Point*. Wired. https://www.wired.com/story/medtronic-insulin-pump-hack-app/

Phillips, C. (2018). The Golden State Killer investigation and the nascent field of forensic genealogy. *Forensic Science International: Genetics, 36,* 186-188.

Ravenscraft, E. (2019, June 12). *How to Protect Your DNA Data Before and After Taking an at-Home Test*. The New York Times. https://www.nytimes.com/2019/06/12/smarter-living/how-to-protect-your-dna-data.html

Robertson, A. (2020, April 10). *How you'll use Apple and Google's coronavirus tracking tool. The Verge*. https://www.theverge.com/2020/4/10/21216715/apple-google-coronavirus-covid-19-contact-tracing-app-details-use

Roehr, B. (2018). Earl Bakken: Founder of Medtronic. *BMJ, 363*, BMJ, 05 November 2018, Vol.363.

Selk, A. (2018, April 26). *All We Know about Joseph DeAngelo, the Golden State Killer Suspect Who Became a Suburban Grandfather*. The Washington Post. www.washingtonpost.com/news/post-nation/wp/2018/04/26/joseph-deangelo-golden-state-killer-suspect-was-normal-grandpa-according-to-teen/?noredirect=on&utm_term=.95dac57e9e0d

Shi, X., & Wu, X. (2017). An overview of human genetic privacy. *Annals of the New York Academy of Sciences, 1387*(1), 61-72.

Sorrel, C. (2008, March 12). *Scientists Demonstrate Deadly WiFi Pacemaker Hack.* Wired. https://www.wired.com/2008/03/scientists-demo/

The 7 Greatest Advantages of Smart Home Automation. (2016, June 14). BlueSpeed AV. https://bluespeedav.com/blog/item/7-greatest-advantages-of-smart-home-automation

The security and privacy issues that come with the Internet of Things. (2020, January 6). Business Insider. https://www.businessinsider.com/iot-security-privacy

Truog, R., Kesselheim, A., & Joffe, S. (2012). Research ethics. Paying patients for their tissue: The legacy of Henrietta Lacks. *Science (New York, N.Y.), 337*(6090), 37-38.