An Actor Network Based Examination of the Healthcare Cybersecurity Crisis

A Research Paper Submitted to the Department of Engineering and Society

In STS 4600
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, Computer Science

By

Gabriel Edwards

Spring 2022

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISORS

Sean Ferguson, Department of Engineering and Society

Rosanne Vrugtman, Department of Computer Science

Daniel G. Graham, Department of Computer Science

Introduction

Healthcare's Cyber-Security Crisis

Imagine that you've suffered a terrifying, life threatening injury and have just been taken to the only hospital within 20 miles, only to be met with the horror of being denied care; the next clinic is so far that the doctors there just can't save you. This was the terrifying real experience of a woman who, in September of 2020, sadly died after being turned away from the Dusseldorf University hospital in Germany. The reason: they had fallen victim to a ransomware attack the week prior. Over two dozen servers of patient information had been encrypted, causing major computer system crashes and crippling the hospital (Associated Press, 2020).

Though deaths resulting directly from ransomware attacks on hospitals are rare, the attacks themselves are anything but. In the U.S. alone during 2020, over 600 healthcare facilities were attacked (Horowitz, 2021), a number that both would double in 2021 (Bilyeau, 2021), and was up 42% from just the year prior (Culbertson, 2021). The goal of these attacks is typically to collect large amounts of highly valuable healthcare records; between just 2009 and 2021, as many as 78 million individual records had been breached in attacks (HIPAA Journal, 2021). These attacks aren't just wide reaching. Apart from potentially ruining computer systems, these attacks can cost a single hospital upwards of 7 million dollars, a potentially disastrous amount for small and rural hospitals (Jalali & Kaiser, 2018). This is to say nothing of the stress and headache caused to patients whose medical and financial data are stolen (Coventry & Branley, 2018), or of the thousands of patients who are denied medical services due to when a hospital loses system access (Poulsen et al., 2021). With the incredible prevalence of and danger posed by these cyber-attacks, the question must be asked: why is it so easy, apparently, to hack hospital networks? To answer this question, I use the Actor-Network Theory to frame hospital networks as a web of devices, human users, and organizations, and trace protected health information through this web. I analyze the interactions

between these actors to look for potential vulnerabilities, and use major concepts of ANT to suggest meaningful solutions

The Inherent Complexity of Hospital Networks

Some of the ease with which these networks are hacked is likely due to the value of the target data: according to findings by Coventry & Branely (2018), "healthcare data is substantially more valuable than any other data," with sets of medical credentials fetching more than a thousand dollars. This value likely attracts a significant number of hackers to hospital networks, increasing the total man-hours thrown at them, and as a result the frequency of successful attacks. Unfortunately, this answer is only one facet of what's widely pointed to as the main cause of these networks' high vulnerability: their overwhelming complexity (Jalali & Kaiser, 2018). Hospital data networks are just too vast.

One of the largest sources of complexity comes from the devices connected to the network, primarily, the sheer amount of them. A cybersecurity officer at one hospital reported there being over 12,000 smartphones and tablets in their network brought by staff; another reported having over 800 "families of medical devices" on their network, with likely dozens to hundreds of any given device type (Jalali & Kaiser, 2018). This is not even considering the size of a hospital's hardwired computer network. All it takes is a single vulnerable device to compromise a network, and any one of these tens of thousands could be. Additionally, many of the connected medical devices just aren't designed with security in mind, leaving very little that can even be done by officials to secure them (Jalali & Kaiser, 2018). Another source of complexity, patient centered spending, makes this network worse (Institute of Medicine, 2001). A hospital's main focus is patient care, so administrators prioritize spending on that; security departments aren't budgeted much, so they're often small (Coventry & Branley, 2018). This also often leaves hospitals stuck with legacy computer systems that are no longer supported (Coventry & Branley, 2018).

Another sizable source of complexity lies in the device's users: hospital staff themselves. Doctors and nurses often see security protocol as barriers to patient care, and as such tend to ignore those behaviors where possible (Jalali & Kaiser, 2018). This is compounded by a careless use of devices, including losing sensitive smart devices and clicking on (many) phishing emails (Jalali et al., 2020). Government regulations placed on hospitals introduce even more complexity, primarily by creating minimum security and data privacy standards (Statchel & DeLaHaye, 2015). These allow security officials to secure a base level of support from hospital administrators, while at the same time forcing them to focus on practices that may not be useful for their specific organization.

Already, the problem of healthcare-data security is very complicated. Even considering only the few complexities covered here, one can see a very wide range of influences, each introducing its own swath of vulnerabilities. The full picture still is much more intricate than can be expanded upon here. This complexity goes a long way to explain the great difficulty hospitals face in dealing with their security vulnerabilities. Deciphering and understanding this complexity, therefore, is crucial to developing meaningful solutions.

Applying The Actor-Network Theory to Healthcare Data

Introduction of Actor-Network Theory and its Application to Cybersecurity

Science and technology studies (STS) principals suggest the use of analytical frameworks to make sense of complicated sociotechnical systems; healthcare data networks certainly qualify, so an appropriate framework should be chosen. Research conducted by Dr. Myriam Cavelty (2018), a senior securities studies lecturer at the University of Zurich, considering the broader field of cybersecurity, suggests the Actor-Network Theory (ANT) to be pertinent. Dr. Cavelty considers both the material insecurities of technologies and the social practices of humans (regarding vulnerabilities) to be equally impactful to cybersecurity. As such, she envisions cybersecurity as a

sort of network, comprising both devices and their human users in equal significance, where vulnerabilities arise from the various interactions between actors. She offers ANT as the obvious choice to analyze this network, as it's specifically useful for examining the depunctializations (breakdowns of routine) in the relationships between actors - these depunctializations are the sources of vulnerabilities. This applies perfectly to healthcare data networks, where even more complexity arises from the relationships between actors than from the many sources already discussed. Analyzing these relationships with ANT will be the best way to discover, and improve, insecurities.

As an aside, ANT not only describes that networks and relationships should be examined, but also provides guidelines for conducting this process (Ritzer, 2004). These guidelines come in the form of three constructs, each of which are meant to conform one's thinking to the principles of ANT, so as to more efficiently arrive at best-practice solutions. The first of these is *agnosticism*, which declares all actors in the network as impartial, and therefore equal to one another in importance and goal. The second is *generalized symmetry*, which suggests that there should be some common language imparted onto all actors, or a single frame that is used to interpret them from a shared baseline. The final is *free association*, which declares all a priori assumptions about the network or its actors should be abandoned. These constructs will serve as the guide for ANT analysis conducted later.

Primary Previous Research Applying ANT to Hospital Data Networks

Conveniently, an Actor-Network examination of healthcare security breaches has already been made by Richard Stachel and Marilyn DeLaHaye (2015), researchers from Robert Morris University, which will form a basis for the research conducted in later sections. Their research aims to investigate the many causes of vulnerabilities leading to the theft of patient health information (which they referred to as Protected Health Information or PHI), and to determine ways of securing

them. It concerns investigating the web of entities and devices involved in the transfer of PHI (dubbed the PHI Network), and applying ANT to look for depunctualizations, weaknesses in relationships between its actors, that lead to major vulnerabilities. The PHI network is based on *theDataMap*™, shown in Figure 1, which is a chart created by Harvard researchers representing the flow of patient health data between the various actors who handle, transfer or dictate it. It is important to note, however, that *theDataMap*™ is not the full picture of the PHI Network. Many of the individual actors are left as *black box* actors which contain their own actor-networks, such as the "Physician, Hospital" actor (Figure 1), which encapsulates nearly all of the sources of complexity described in the previous section. These sub-networks are used and considered in the authors examination of the PHI Network, but are never expanded upon explicitly.

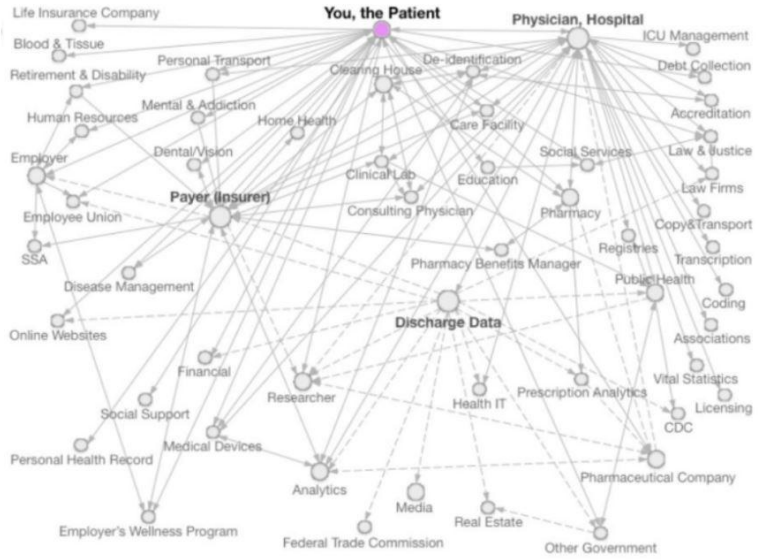

Figure 1. theDataMap™

Statchel's & DeLaHaye's (2015) application of ANT to the PHI network is used primarily to offer solutions to what they have determined to be the three major sources of vulnerabilities within the network. ANT is used in two major ways to address these three vulnerabilities: firstly, as inferred from the authors use of actors and actor relationships as the basis of the solutions, it's used

to find relevant relationships in the network which can be modified to affect positive change. A given vulnerability is broken down into the individual actors (more accurately types of actors, as in staff instead of physicians specifically) either involved or directly responsible, and then each of their relationships within the network are evaluated for their potential effect on the vulnerability. As an example, consider hospital staff's propensity for losing sensitive devices (Statchel & DeLaHaye, 2015): that actor's relationship to hospital administrators might have a high potential for positive change, as administrators could increase training, strengthen disciplinary actions, or offer incentives. The second major application of ANT is in determining particular, effective changes to the high-potential relationships that are found. When searching for viable solutions for a given actor, the authors use each of the three constructs of ANT (agnosticism, generalized symmetry, and free association) as a guideline; looking for a solution that conforms agnosticism both limits the breadth of one's search, and increases the likelihood that it will be effective.

Methods of Expanding Upon Previous Research

Stachel's and DeLaHaye's (2015) work is an excellent examination of health-data network vulnerabilities, and forms a strong foundation for research applying ANT to these systems. In the years following its publication, however, the landscape of electronic health-data has seen a dramatic shift. Their research suggests that at the time, patient involvement with health-data, like accessing medical records online, was only just beginning to gain popularity (p. 189-190); as such, patients were not considered as a part of the network, or factored into any analysis. This has changed dramatically in more recent years, after the Covid-19 pandemic saw the need for online medicine solutions skyrocket globally (Meyer, 2020). In the first three months alone, use of telehealth services soared by as much as 80% (Bestsennyy et al., 2021), with millions of patients using web portals and services to conduct appointments, communicate with providers, and view health data (Karimi et al., 2021). The pandemic has also seen interest in remote patient monitoring increase

substantially, where medical devices are used to collect data on patient vitals in the home and report them to doctors via the internet (Siwicki, 2022). This is coinciding with both an expansion of internet connectivity in implantable medical devices (Hassija et al., 2021) and the recent boom in personal health monitoring wearables, like fitness trackers and smart health watches (Phaneuf, 2022), leading to an explosion of mobile medical devices (MMDs) connected to hospital networks.

The widespread adoption of telehealth services has led to tens to hundreds of millions of new people and devices interacting with healthcare data systems, expanding these networks' surface area for potential attacks nearly exponentially (Jalali et al., 2020b). The expansion of MMD use has a similar effect, while also introducing many new and different physical vulnerabilities inherent to the devices (Kaspersky, 2022). These developments represent a radical evolution of the PHI Network considered by Stachel and DeLaHaye (2015), with the addition of new actors related to them (primarily patients, telehealth vendors and MMDs) . The aim of this research, therefore, is to expand upon and modernize their original work by using this updated PHI Network to examine the primary vulnerabilities specifically introduced by these new actors. ANT is applied to these vulnerabilities in the same manner as Stachel's and DeLaHaye's work, as both a means of discovering depunctualizations and a lens with which to explore potential solutions to them.

Expanding Upon The New Actors to the PHI Network

The Significance and Vulnerability of Telehealth Related Actors

Historically, patients have had little to no opportunity to engage with electronic health records (EHRs); it wasn't until 2010, with the Obama administration's passing of the HITECH and Affordable Care Acts, that healthcare organizations saw any incentive (Blumenthal & Tavenner, 2010). Even as recently as 2015, only 10 percent of U.S. hospitals provided adequate access to online services for patients (Garrido et al,, 2016). The later half of the 2010's saw a more significant

increase in patient engagement, however: by the end of 2019, the Health Information National Trends Survey found that as many as 60% of patients were offered access to a patient portal, and as many as 40% of those individuals actually accessed them (HealthIT, 2021). These patient portals act as the primary means for patients to access their EHRs, and connect with hospital networks to schedule appointments, communicate with physicians, and pay bills (Glausser, 2020). Nearly overnight, however, the Covid-19 pandemic in 2020 forced a global shift towards the use of telehealth, with the first three months alone seeing over half of all Medicare physician visits occurring online - up from .01 percent (Hartwig, 2021). Though it's use has leveled off (at 380% higher than 2019) two years later, telehealth, which encompasses virtual hospital visits and patient portal use, is anticipated by experts to be a permanent service, with as many as two thirds of patients expressing a desire for post pandemic virtual access (Fauteux, 2022).

With over 50 million telehealth hospital visits occurring in just the Medicare network in 2020 alone, there have likely been hundreds of millions of patients accessing telehealth in the two years since, many likely interacting with EHRs. There's little doubt that it has a substantial effect on the vulnerability of the PHI Network (Hartwig, 2021). PHI leaks through online portals have been a known occurrence since at least 2019: member portal hacks of two separate Blue Cross organizations occurred in in 2019 (Davis, 2019) and 2020 (Davis, 2020), and at least one third party patient portal vendor was breached since the pandemics start (Davis, 2021). Additionally, cyber-security reporting agency DarkOwl found that telehealth vendors in 2020 as a whole suffered a 117% increase in attempted attacks, with at minimum tens of thousands of PHI stolen from them per month - largely due to poor web application security (DarkOwl, 2021). Their findings suggested a systematic shift in attackers' focus (at least partly) away from traditional hospital networks, to these telehealth vendors.

Connecting Telehealth Actors to the PHI Network

Telemedicine related vulnerabilities arise from a variety of sources, and connect to various actors within the traditional PHI Network. The flow of telehealth related PHI starts with patients, who are interfacing with the PHI Network entirely through internet services on computers and smart devices. Patients might view their PHI by interacting with providers' existing EHR databases through patient portals (Mayo Clinic, 2020). These portals may be supplied by the provider directly (Meyer, 2020), or by the third party vendor used by the provider to store EHRs, like the Epic MyChart. Health data is also entered by patients into the network in a variety of ways: over email services; through telehealth vendors web apps, over text chats and video/audio calls, as well as by entering it directly into their databases; and through personal health and wellness apps, which may connect to existing EHR databases (Mayo Clinic, 2020).

Data provided through email travels directly to physicians, interacting only with the email servers and the hospital staff who receive and/or review it. Data provided through telehealth vendors interacts first with their web applications, whether it's either given verbally during a synchronous physician visit (Jalali et al., 2020b), or entered directly into the application for a physician to review asynchronously. From there, PHI is often stored in a server held by the vendor, both as recordings of visits and data entered directly (Privacy International, 2021); data entered directly for is then either transferred to a hospitals EHR network, or accessed directly from their service for physician review (Mayo Clinic, 2020). Data collected by personal health and health monitoring apps similarly is stored in their databases, and sometimes transferred to a hospital's EHR network. PHI provided to both telehealth services and personal health apps have also been known to be shared with various outside parties in the private sector (Privacy International, 2021). Primarily, PHI entered to the existing network by patients, through whatever means, primarily interfaces with physicians/staff; from there however, it will flow through the network in the same manner as traditionally entered EHRs.

All of the actors involved in telehealth introduce unique vulnerabilities to the PHI Network. Patients provide a large source of complexity, as they're prone to the same careless device use that physicians are; they're just as likely to fall victim to phishing scams, or use insecure passwords, or lose devices. Unlike hospital staff, however, patients are not subject to organizational cyber-security protocols, or necessarily provided cyber-security training. As well, the devices used by patients to access EHRs cannot be physically secured or monitored by IT personnel, and may well be connected to insecure networks. There may be millions of patients connected to an EHR database, and a hacker can access all of their PHI with only a single stolen login (Torrence, 2021). Telehealth vendors themselves introduce significant vulnerability, primarily through the poor security of their web applications, which can be directly hacked (DarkOwl, 2021). As well, they are known to store amounts of PHI far exceeding that held in hospital EHR networks, intensifying the severity of their attacks (Sullivan, 2020). Hospital staff also add to telehealth insecurity, in the same ways that they introduce vulnerabilities to hospital networks (Davis, 2020).

The Significance and Vulnerability of Mobile Medical Device Actors

Mobile Medical Devices (MMDs) is a term used in this research to denote certain internet connected (or Internet of Things, IoT) medical devices that are either wearable or implanted. Implanted medical devices are gadgets that are embedded within a patient's bodies to monitor or improve their health, like pacemakers and insulin pumps. Increasing amounts of these devices are now being built with some form of wireless internet connection, enabling continuous health feedback and various remote control functionalities. (Emergo, 2019). Wearable devices are meant to non-invasively gather health-related data from users, including things like heart rate and levels of blood glucose and oxygen (Dolan, 2022). Largely these have taken the form of consumer health and fitness trackers, like Fitbit and other smart-watches, which record simple health information like heart rate and temperature for personal use (Dinh-Le et al., 2019). These devices have become

extremely popular and widespread over the past decade, with 78 million users in 2021 (Phaneuf, 2022), and are by far the most common MMDs. Remote patient monitoring (RPM) devices are a second type of wearable, and are used to collect health data from patients outside of a clinic setting, and electronically send it to physicians (Dolan, 2022). They are capable of collecting wider varieties of data than personal trackers, and are able to monitor things like blood glucose, gait, and atrial fibrillation (Dunn et al. 2018).

Internet connected MMDs are a relatively new technology, with the first wireless pacemaker having been implanted in 2009 (Ashford, 2009), but are increasingly and quickly becoming more popular. Advancements in technologies like materials science, batteries, computers, and data transmission allow these devices to become smaller, sense more accurate data, and send data faster every year (Guk et al., 2019). As these devices grow more capable, they are adopted by healthcare more and more. For instance, there were over 400 wearable devices compatible with EHR in 2019 (Dinh-Le et al., 2019), just 10 years after the first IoT pacemaker, and implanted devices' percentage of the global medical IoT market share more than doubled between 2017 and 2020 (Jayah, 2019). Personal fitness trackers have also seen increasing use in healthcare as RPM devices, with integration into various EHR platforms (Dinh-Le et al., 2019) and advances in sensing capabilities, like the addition of ECG sensing in the 2021 Apple Watch. The growth of MMDs is not expected to slow down any time soon. Between promising research tackling historic technological problems, like real time data transmission (Wang et al, 2022), increasing belief in their benefit to chronic illness care (Hassija et al., 2021), and the Covid-19 pandemic seeing calls for RPM solutions skyrocket (Siwicki, 2022), MMDs are expected to become a 50 billion dollar industry by 2030.

The growth of MMDs represents a massive vulnerability increase to the PHI Network. In addition to increasing its attack surface area exponentially, these devices are known to be riddled with vulnerabilities, and extremely easily hackable. This is especially true in implanted devices, as

their size limits computing power and memory, making it difficult to implement security measures (McGowan et al., 2021); hundreds of thousands of devices of all kinds have been recalled due to insecurities (Hassija et al, 2021). A hacked pacemaker could not only be used to kill (very easily), but also as a backdoor into its connected hospital network to steal PHI and install malware (Jaret, 2018). As well, wearables connected to EHR databases could expose PHI directly to hackers; the protocol used by many of them to transmit data has been shown just this year to contain 33 vulnerabilities (Kaspersky, 2022).

Despite the fact that no cyber attacks directly attributed to MMDs have yet been reported (McGowan et al., 2021), their effect on the PHI Network is no less important than any other source of vulnerability. The Covid-19 pandemic has seen remote patient monitoring put to the test all over the country, and the positive results seen (Csale et al., 2021) are causing a greater push than ever for a general integration into healthcare (Gowda et al, 2022). This increase in interest brings with it an increase in research, and a much higher potential for historic barriers to MMDs, like battery life and accuracy (Pearne, 2021) to be overcome. Considering these on top of the meteoric rise in use MMD have already experienced over the past decade (Iqbal et al., 2021), there's ample reason to believe they may become ubiquitous in the coming years (Philipson, 2021). Considering the current heavy use of standing IoT medical devices as attack vectors (Khera, 2017), it's only a matter of time before this increasing number of highly insecure mobile devices is capitalized on; applying ANT to help prevent this is just as vital as defending current threats.

Connecting MMD Actors to the PHI Network

Currently, integration of MMDs to the PHI Network is fairly direct. For all MMDs, all of the PHI involved originates from the device, as that is their specific function, and they have no reason to receive PHI. For implanted devices, collected data is either sent directly to physicians during in-clinic visits, or sent automatically to the manufacturer through a home transmitter device; data

sent automatically is then sent directly to physicians (Burri, 2013). For wearables, the process is similar: due to current technical limitations, PHI collected by these devices, in addition to any local storage on the devic, are sent directly to proprietary smartphone applications (Yetisen et al., 2018). Therefore, PHI collected by these devices are stored in manufacturer data bases, where it can then be sent to physicians, through direct integration with hospital EHR databases (Dinh-Le et al., 2019). As with telehealth actors, MMDs primarily interface with the PHI Network through physicians/staff, and from there, it will flow through the network in the same manner as traditionally entered EHRs.

Despite the directness of PHI flow involving MMDs, there are ample opportunities for vulnerabilities to be introduced. Primarily these stem from insecurities inherent to the devices: they can be easily hacked either directly, to allow for direct access to hospital networks, or as data is sent to mobile devices (Jaret, 2018), through transmission protocol vulnerabilities (Kaspersky, 2022). These insecurities are exacerbated by patient actors, who may either venture into unsecured networks, or even inadvertently install malware directly onto the computers or mobile devices that their MMDs connect to. Manufacturers may also introduce vulnerabilities, as the applications that collect data from MMDs may be, and have been, hacked to leak PHI (Horowitz, 2021). Interestingly, manufacturers also have been shown to leak PHI intentionally, by selling it directly to third parties (Yetisen et al., 2018).

ANT Based Analysis of Major Sources of Vulnerability Within the PHI Network

Identifying Major Vulnerabilities

In this section, the major sources of vulnerability added to the PHI Network by the widespread adoption of telehealth and mobile medical devices that have been identified are discussed. This is done in a similar manner to the identification of primary vulnerabilities within the original PHI Network by Stachel and DeLaHaye (2015). For reference, these were given as: the

sheer amount of electronic data available and the incredible number of devices connected to it; an increasing number of stationary medical devices capable of internet connection; and large scale human irresponsibility with PHI, such as staff losing sensitive devices and falling for phishing scams.

The advance of both telehealth and MMDs alike increase the surface area for attacks by an extreme amount, thanks to their unprecedented increase in both PHI collection and number of connected devices. In 2016, there were an estimated 1.14 million permanent pacemakers in use globally (Mevissen, 2018) - only one of dozens of different implanted IoT devices (Alvarado, 2018). Combined with the estimated 45 million patients using RPM devices per year, and the unknown portion of over 84 million fitness trackers in 2022 connected to EHR (Phaneuf, 2022), the amount of MMDs in use dwarfs the estimated 10-15 million standing devices across all U.S hospitals (Miliard, 2016). This is to say nothing of the *at bare minimum* equal number of connected applications *and* devices connected to store their data, or the *many* patient portals, independent telehealth apps, and devices connected to the estimated 120 million U.S telehealth visits in one year alone (Michas, 2021; Charleson, 2022). Additionally, this unprecedented number of devices and software, a number expected to grow yearly, is responsible for generating untold amounts of new PHI; copies of which are stored in countless manufacturer databases that have been breached in the past (McKeon, 2021).

Aside from the sheer number of these devices and applications, and data transfers between them, their inherent vulnerabilities create a massive problem for PHI security. Implanted devices, for instance, have seen numerous potentially catastrophic vulnerabilities demonstrated, with the FDA having recalled 465,000 pacemakers and 350,000 implanted defibrillators between 2017 and 2018 alone (Hissaj, 2021). The software in question is also far from secure: a single study in 2021 testing 30 mobile health apps, including apps from mobile health vendors and large hospital

systems alike, found every single one to be vulnerable to hacks directly through their program interfaces (Horowitz, 2021); at least one in particular allowed direct access to a hospitals EHR database. In addition to their commonality and severity, these vulnerabilities pose several unique, new challenges. It's widely known that standing medical devices are typically manufactured without any care towards security, but the size of implantables adds to this by making it *difficult* to add things like encryption (Rasool et al., 2022). As well, all of these devices and software are meant to be accessed outside of any hospital internet networks. So not only are they connected to, and transfering data through, unknown and unsecured wifi networks (Hassija, 2021), but they're also outside of any organizational oversight; an IT security officer can't vet a patient's computer for malware.

Finally, expanding upon another major vulnerability of the original network, human misuse and irresponsibility, specifically with the addition of patients to the PHI Network, is potentially the most dangerous insecurity of all. Patients are *at least* just as likely as hospital staff to lose sensitive devices (like personal phones connected to EHR) and fall victim to a phishing scam; both of these cities at different points in time as the most common healthcare cyber-attack vectors (Stachel & DeLaHaye, 2015; Coble, 2022). They also, however, provide challenges that are totally unique from staff. To start, the primary solutions suggested for hospital staff, training and increased accountability, are not feasible to apply to patients: hospital actors have no authority over patients, and cannot enforce any measures. As well, the personal devices used by patients to access telehealth and rpm software are not used within a hospital's network; they can't be protected from malware by security officers, and their wifi network may be unsecured.

Applying ANT to the PHI Network to Suggest Meaningful Solutions

In this section, the primary vulnerabilities identified within the PHI Network are addressed, using Actor-Network Theory to establish meaningful changes to the relationships of the actors

involved. The three constructs of ANT previously defined are used as a basis in determining these changes, and they are used to organize the presentation of these suggestions. This method of analysis carries from that of Stachel's and DeLaHaye's (2015) previous work.

The first ANT construct is agnosticism, which emphasizes the equal actions of all actors for the good of the network, in this case the protection of PHI. The primary and simplest manifestation of this has to do with manufacturers and vendors building their devices and software more securely. Though this sounds highly reductive, a common theme throughout the literature is the surprising amount of obvious and easy to fix vulnerabilities that fly right in the face of patient security. These include things like device manufacturers using outdated libraries with known bugs (Khandelwal, 2017); healthcare organizations creating portals with traditional and insecure single factor and email authentication, despite multi-factor being more secure and as easy to implement (Bertoncini, Jackson, 2019); and vendors choosing not to encrypt databases, despite it taking nearly no work.. Actor behaviors like these, that require no additional oversight to correct, simply must be changed.

Additionally, similarly to Statchel's and DeLayHe's (2015) application of agnosticism, it requires the recruitment of new actors with crucial new abilities that can add security to the system. Importantly, this involves finding experts to create effective learning materials to train patients using telehealth and MMDs in proper cyber-security behaviors (Dinesen et al., 2016). Research has shown a direct correlation between proper training and reducing cybersecurity incidents, and this is an area where providers currently struggle (Dinesen et al., 2016). Another area severely lacking capable actors is active threat monitoring, which has been suggested to aid in defending data storage platforms, finding freshly developed attacks against devices (Rasool et al., 2022), and blocking unauthorized device access to patient portals (experian health, 2019).

Finally, agnosticism suggests a strengthening of inter-actor relationships, particularly building communication between stakeholders (McGowan et al., 2021). A 2022 survey of

cybersecurity experts suggests that many medical device users, as well as the medical staff training these patients, are unaware of their security functions and risks (Deal & Sambasivam, 2022). As end users have been identified as the targets of 95% of attacks (Deal & Sambasivam, 2022), strengthening communication between device manufacturers and physicians, as well as between physicians and patients, is likely to promote an increase in device security.

Generalized symmetry promotes the use of common language amongst actors, which takes the form here of regulation and process standardization. Firstly, government legislation has played a large role in securing PHI up to this point, with the HITECH act enforcing patient data security and HIPPA requiring the reporting of data breaches (Rasool et al., 2022). Regarding medical devices, however, the main form of regulation comes from the FDA, which focuses on pre and post production guidelines, which concern security labeling, and security requirements (McGowan et al., 2021). As such, it's recommended that some form of regulation regarding minimum hardware and software security requirements be passed, so as to standardize the MMD industry. Another necessary network standardization is the concept of interoperability, which is the idea of creating a common language amongst all medical device (wearables, stationary, implantables), EHR databases, telehealth services, to seamlessly integrate all medical data (Gowda et al.,, 2022). As it stands, without standardization, competition amongst vendors and manufacturers creates both a myriad of devices with heterogeneous data transfer standards that don't combine seamlessly, and countless copies of data across various device-specific databases (Rasool et al., 2022). A reduction in this massive endpoint complexity would solve various issues in privacy, security, and authentication. Finally, it's suggested that healthcare organizations standardize the internet networks of all remote devices attempting to transmit data to the PHI Network; one possibility is to require all devices connect through a VPN, to sidestep potential insecurities (O'Dowd, 2016).

The expectation of free association, the final ANT construct to reject primary assumptions regarding the PHI Network. An assumption widely held throughout the network is that computers are laptops, desktops, and mobile devices; when people think of vulnerabilities, they often don't consider IoT devices, and certainly not the small mobile devices (Marchang et al., 2019). This is a dangerous assumption, which leads to the security of these devices being largely ignored (Rasool et al., 2022), despite the knowledge that many medical devices have already been healthcare breach vectors. This assumption must be dropped in favor of increased research into MMD security, and adoption of regular device screenings, before hackers notice the opportunity inherent to these devices. As well, organization heads need to stop seeing cyber-security as only a financial loss, and instead see it as investing in greater loss prevention (Marchang et al., 2019). Very little money is put towards network security efforts across the board, leading to the miniscule effort put into device, application, and database security seen today. Finally, the idea that shipping medical devices riddled with vulnerabilities has no place in the modern IoT landscape. Given the size constraints of MMDs, security is often sacrificed for performance, for the sake of selling the devices sooner, or more cheaply (Rasool et al., 2022). Given the vastness of IoT today, and the commonality of healthcare cyber attacks, the lives make up more and more of the risk involved every year.

Conclusions

Moving well into the second decade of a true public health crisis, a larger number of hospitals are attacked, and more personal health information is stolen, each year than the one before; even the Covid-19 pandemic couldn't break this trend (Evans, & McMillan, 2021). This paper first asked the question why, and determined an unsettling reason: patient health data is like gold, and hospital data networks are so overwhelmingly complex that it becomes laughably easy to steal (Akpan, 2016). After determining that the Actor-Network Theory is the best method to untangle this complexity, and that it had already been used to analyze the major sources of vulnerability

inherent to healthcare data (Stachel, & DeLaHaye, 2015), this paper's main concern was modernizing this approach. That is, the network was re-analyzed to determine the effects of both recent technological advancements in medical devices and the Covid-19 pandemic on healthcare cyber-security. While it was determined that they both drastically increase the insecurity of healthcare data, ANT analysis conducted showed great promise in allowing effective solutions to this insecurity to be found.

References

Alvarado, J. (2018, September 14). *The IoT within us: Network-connected medical devices.* Synopsys. https://www.synopsys.com/blogs/software-security/network-connected-medical-devices/

Akpan, N. (2016, March 23). *Has health care hacking become an epidemic?* PBS NewsHour. https://www.pbs.org/newshour/science/has-health-care-hacking-become-an-epidemic

Ashford, M. (2009, August 11). *First Internet-Connected Pacemaker Successfully Implanted.* Popular Science. https://www.popsci.com/scitech/article/2009-08/first-patient-implanted-pacemaker-communicates-wirelessly-her-doctor/#:~:text=Wireless%20Pacemaker-,The%20first%20American%20to%20be%20implanted%20with%20a%20wireless%20pacemaker,by%20the%20FDA%20in%20July.

Associated Press. (2020, September 17). *German hospital hacked, patient taken to another city dies.* NBC News. https://www.nbcnews.com/?icid=nav_bar_logo

Bestsennyy, O., Gilbert, G., Harris, A., & Rost, J. (2021, July 9). *Telehealth: A quarter-trillion-dollar post-COVID-19 reality?* McKinsey & Company.

Bilyeau, N. (2021, August 18). *Newest Target of Cyber Attacks: America's Hospitals*. The Crime Report. https://thecrimereport.org/2021/08/18/hospitals-cyberattacks/

Blumenthal, D., & Tavenner, M. (2010). The "Meaningful Use" Regulation for Electronic Health Records. *The New England Journal of Medicine.* https://www.nejm.org/doi/full/10.1056/NEJMp1006114

Burri, H. (2013) Remote follow-up and continuous remote monitoring, distinguished, *EP Europace. 15(1)*. https://doi.org/10.1093/europace/eut071

Cavelty, M. (2018). Cybersecurity Research Meets Science and Technology Studies. *Politics and Governance. 6(2)*. 22-30 https://www.cogitatiopress.com/politicsandgovernance/article/view/1385/1385

Charleson, K (2022, January 20). *Telehealth statistics and telemedicine trends 2022.* The Checkup. https://www.singlecare.com/blog/news/telehealth-statistics/

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas. 113.* 48-52 https://www-clinicalkey-com.proxy01.its.virginia.edu/#!/content/journal/1-s2.0-S0378512218301658

Casale, P. N., Vyavahare, M., Coyne, S., Kronish, I., Greenwald, P., Ye, S., Deland, E., & Fleischut, P. M. (2021). The Promise of Remote Patient Monitoring: Lessons Learned During the COVID-19 Surge in New York City. *American journal of medical quality : the official journal of the American College of Medical Quality,* 36(3), 139–144. https://doi.org/10.1097/01.JMQ.0000741968.61211.2b

Culbertson, N. (2021, June 7). *Increased Cyberattacks On Healthcare Institutions Shows The Need For Greater Cybersecurity*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2021/06/07/increased-cyberattacks-on-healthcare-institutions-shows-the-need-for-greater-cybersecurity/?sh=60fc75985650

DarkOw (2021). *Listening to Patient Data Security: Healthcare Industry & Telehealth Cybersecurity Risks.*

https://securityscorecard.pathfactory.com/all/healthcare-industry-telehealth-cybersecurity-risks-report

Davis, J. (2019, April 16). *Hackers Breach Blue Cross of Idaho Provider Portal in Fraud Attempt.* Health IT Security. https://healthitsecurity.com/news/hackers-breach-blue-cross-of-idaho-provider-portal-in-fraud-attempt

Davis, J. (2020, July 7). *Magellan Health Data Breach Victim Tally Reaches 365K Patients.* Health IT Security. https://www.google.com/url?q=https://healthitsecurity.com/news/magellan-health-data-breach-victim-tally-reaches-365k-patients&sa=D&source=docs&ust=1650824355979365&usg=AOvVaw2E6fDWuuDFxNlxvRJlKwza

Davis, J. (2021, November 5). *Cyberattack on health tech vendor QRS leads to data theft tied to 320K patients.* HSC Media. https://www.scmagazine.com/analysis/breach/cyberattack-on-health-tech-vendor-qrs-leads-to-data-theft-tied-to-320k-patients

Deal, J. & Sambasivam, S. (2022). Security Control Techniques: Cybersecurity & Medical Wearable Devices. *Journal of Information Systems Applied Research. 15(1).* ISSN: 1946-1836

Dinesen, B., Nonnecke, B., Lindeman, D., Toft, E., Kidholm, K., Jethwani, K., Young, H. M., Spindler, H., Oestergaard, C. U., Southard, J. A., Gutierrez, M., Anderson, N., Albert, N. M., Han, J. J., & Nesbitt, T. (2016). Personalized Telehealth in the Future: A Global Research Agenda. *Journal of medical Internet research. 18(3).* https://doi.org/10.2196/jmir.5257

Dinh-Le, C., Chuang, R., Chokshi, S., & Mann, D. (2019). Wearable Health Technology and Electronic Health Record Integration: Scoping Review and Future Directions. *JMIR mHealth and uHealth, 7(9)*. https://doi.org/10.2196/12861

Dolan, S. (2022, January 15). *The technology, devices, and benefits of remote patient monitoring in the healthcare industry.* Insider Intelligence. https://www.insiderintelligence.com/insights/remote-patient-monitoring-industry-explained/

Dunn, J., Runge, R., & Snyder, M. (2018). Wearables and the medical revolution. *Future Medicine. 15(5).* https://doi.org/10.2217/pme-2018-0044

Is your patient portal as secure as it should be? (2019). Experian Health. https://www.experian.com/content/dam/marketing/na/healthcare/brochures/how-patient-portals-get-hacked.pdf

Evans, M. & McMillan, R. (2021, February 26). *Cyberattacks Cost Hospitals Millions During Covid-19.* The Wallstreet Journal. https://www.wsj.com/articles/cyberattacks-cost-hospitals-millions-during-covid-19-11614346713

Fauteux, N. (2022). The Growth of Telehealth. *American Journal of Nursing. 112(3). doi: 10.1097/01.NAJ.0000822960.95263.e5*

Garrido, T., Raymond, B., Wheatley, B. (2016). Lessons From More *Than A Decade In Patient Portals*. Health Affairs. https://www.healthaffairs.org/do/10.1377/forefront.20160407.054362

Ghafur, S., Kristensen, S., Honeyford, K. *et al* (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. *npj Digital Medicine. 2(98)*. https://doi.org/10.1038/s41746-019-0161-6

Glauser, A. (2020, April 21). *The Evolution of the Patient Portal: Where we are Today.* AdvacncedMD. https://www.advancedmd.com/blog/patient-portal-evolution-today/

Gowda V., Schulzrinne H., Miller BJ. (2022). The Case for Medical Device Interoperability. *JAMA Health Forum. 3(1)*. doi:10.1001/jamahealthforum.2021.4313

Guk, K., Han, G., Lim, J., Jeong, K., Kang, T., Lim, E. K., & Jung, J. (2019). Evolution of Wearable Devices with Real-Time Disease Monitoring for Personalized Healthcare. Nanomaterials (Basel, Switzerland), 9(6), 813. https://doi.org/10.3390/nano9060813

Hartwig, B. *Telemedicine Vulnerabilities Are a Dream Come True for Hackers*. HealthWorks Collective. https://www.healthworkscollective.com/telemedicine-vulnerabilities-are-a-dream-come-true-for-hackers/

Hassija, V., Chamola, V., Bajpaia, B., Zeadally, N. (2021). Security issues in implantable medical devices: Fact or fiction? *Sustainable Cities and Society. 66. https://doi.org/10.1016/j.scs.2020.102552*

Horowitz, B. (2021, March 26). 2020 offered a 'perfect storm' for cybercriminals with ransomware attacks costing the industry $21B. *Fierce Healthcare.* https://www.fiercehealthcare.com/tech/ransomware-attacks-cost-healthcare-industry-21b-2020-here-s-how-many-attacks-hit-providers

Institute of Medicine (US) Committee on Quality of Health Care in America. (2001). *Crossing the Quality Chasm: A New Health System for the 21st Century.* Washington (DC): National Academies Press (US). DOI: 10.17226/10027

Internet of Bodies: What's getting into you. (2019, July 19). *Emergo*. https://www.emergobyul.com/blog/2019/07/internet-bodies-whats-getting-you

Iqbal, S.M.A., Mahgoub, I., Du, E. et al. (2021). Advances in healthcare wearable devices. *npj Flex Electron. 5(9*). https://doi.org/10.1038/s41528-021-00107-x

Jalali, M., &, Kaiser, J. (2018). Cybersecurity in Hospitals: A Systematic, Organizational Perspective. *Journal of Medical Internet Research. 20(5).* https://www.jmir.org/2018/5/e10059/

Jalali, M., Bruckes, M., Westmattelmann, D., & Schewe, G. (2020a). Why Employees (Still) Click on Phishing Links: Investigation in Hospitals. *Journal of Medical Internet Research. 22(1).* https://www.jmir.org/2020/1/e16775?utm_source=TrendMD&utm_medium=cpc&utm_campaign=JMIR_TrendMD_0

Jalali, M., Landman, A., & Gordon, W. (2020b). Telemedicine, privacy, and information security in the age of COVID-19. *Journal of the American Medical Informatics Association. 28(3).* https://doi.org/10.1093/jamia/ocaa310

Jayah, A. (2019, February 18). *Body Talks: The Future of the Connected Implanted Medical Devices Industry.* Speeda. https://asia.ub-speeda.com/en/body-talks-future-connected-implanted-medical-devices-industry/#:~:text=The%20global%20connected%20implanted%20medical,main%20drivers%20of%20industry%20growth.

Jaret, P. (2018, November 12). *Exposing vulnerabilities: How hackers could target your medical devices.* AAMC. https://www.aamc.org/news-insights/exposing-vulnerabilities-how-hackers-could-target-your-medical-devices

Karimi, M., Lee, E., Couture, S., Gonzales, A., Grigorescu, V., Smith, S., De Lew, N., & Sommers, B. (2022). *National Survey Trends in Telehealth Use in 2021: Disparities in Utilization and Audio vs. Video Services*. Report prepared for Assistant Secretary for Planning and Evaluation Office of Health Policy.

Khandelwal, S. (2017, June 5). *Over 8,600 Vulnerabilities Found in Pacemakers.* The Hacker News. https://thehackernews.com/2017/06/pacemaker-vulnerability.html

Khera, M. (2017). Think Like a Hacker: Insights on the Latest Attack Vectors (and Security Controls) for Medical Device Applications. *Journal of Diabetes Science and Technology. 11(2).* https://doi.org/10.1177/1932296816677576

Landi, H. (2022, February 1). Healthcare data breaches hit all-time high in 2021, impacting 45M people. *Fierce Healthcare.* https://www.fiercehealthcare.com/health-tech/healthcare-data-breaches-hit-all-time-high-2021-impacting-45m-people

Marchang, J., Beavers, J., & Faulks, M. (2019). Hacking NHS Pacemakers: A Feasibility Study.IEEE *12th International Conference on Global Security, Safety and Sustainability (ICGS3)* doi: 10.1109/ICGS3.2019.8688214.

Mayo Clinic Staff (2020, May 15). *Telehealth: Technology meets health care.* May Clinic. https://www.mayoclinic.org/healthy-lifestyle/consumer-health/in-depth/telehealth/art-20044878

McKeon, J. (2021, September 16). *61M Fitbit, Apple Users Had Data Exposed in Wearable Device Data Breach.* Health IT Security. https://healthitsecurity.com/news/61m-fitbit-apple-users-had-data-exposed-in-wearable-device-data-breach#:~:text=September%2016%2C%202021%20%2D%20Over%2061,independent%20cybersecurity%20researcher%20Jeremiah%20Fowler.

McGowan, A., Sitting, S., & Andel, T. (2021, January 5). *Medical Internet of Things: A Survey of the Current Threat and Vulnerability Landscape*. [Paper presentation]. Hawaii International Conference on System Sciences, Hawaii, United States. DOI: 10.24251/HICSS.2021.466

Meyer, M. (2020). COVID-19 Pandemic Accelerates Need to Improve Online Patient Engagement Practices to Enhance Patient Experience. *Journal of Patient Experience 7(5).* DOI: 10.1177/2374373520959486

Mevissen, M. (2018, May 16). *Implantable medical devices are becoming increasingly capable.* Ametek Components and Wire. https://www.ametek-coining.com/knowledge/blog/2018/may/implantable-medical-devices-are-becoming-increasingly-capable

Michas, F. (2021, August 10). *Total hospital outpatient visits in the United States 1965-2019.* Statista. https://www.statista.com/statistics/459744/total-outpatient-visit-numbers-in-the-us/#:~:text=Total%20hospital%20outpatient%20visits%20in%20the%20United%20States%201965%2D2019&text=This%20statistic%20displays%20the%20total,hospitals%20located%20in%20the%20country.

Millard, M. (2016, February 29). *Cybersecurity pro: Networked medical devices pose huge risks to patient safety.* Healthcare IT News. https://www.healthcareitnews.com/news/cybersecurity-pro-networked-medical-devices-pose-huge-risks-patient-safety#:~:text=Consider%20these%20numbers%3A%20There%20are,have%201%2C500%20infusion%20pumps%20alone.

Mitchell, K. (2021). Internet of Things-enabled Smart Devices, Healthcare Body Sensor Networks, and Online Patient Engagement in COVID-19 Prevention, Screening, and Treatment *American Journal of Medical Research 8(1).* https://web-p-ebscohost-com.proxy01.its.virginia.edu/ehost/pdfviewer/pdfviewer?vid=5&sid=95774ff7-c219-402a-8f42-9d1e95961bfd%40redis

O'Dowd, E. (2016, August 22). *How Virtual Private Networks Benefit Healthcare Technology.* HIT Infrastructure. https://hitinfrastructure.com/news/how-virtual-private-networks-benefit-healthcare-technology

Office of the National Coordinator for Health IT. (2021, September). Individuals' Access and Use of Patient Portals and Smartphone Health Apps, 2020. https://www.healthit.gov/data/data-briefs/individuals-access-and-use-patient-portals-and-smartphone-health-apps-2020#:~:text=About%20six%20in%2010%20individuals,smartphone%20health%20app%20in%202020

Pearne, N. (2021, July 22). *Reducing noise to improve accuracy of medical devices.* Met-Tech Innovation News. https://www.med-technews.com/

Phaneuf, A. (2021, April 15). *Latest trends in medical monitoring devices and wearable health technology.* Insider Intelligence.

https://www.insiderintelligence.com/insights/wearable-technology-healthcare-medical-devices/

Philipson, B. (2021, September 1). *Life after COVID: Remote patient monitoring will be even more critical.* McKnights Long-term Care News. https://www.mcknights.com/blogs/guest-columns/life-after-covid-remote-patient-monitoring-will-be-even-more-critical/

Poulson, K., McMillan, R., & Evans, M., (2019, September 30). *A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death.* The Wall Street Journal. https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116

Rasool, R., Ahmad, H., Rafique, W., Qayyum, A., & Qadir, J. (2022). Security and privacy of internet of medical things: A contemporary review in the age of surveillance, botnets, and adversarial ML. *Journal of Network and Computer Applications. 201.* https://doi.org/10.1016/j.jnca.2022.103332.

Ritzer, G. (2004). *Encyclopedia of Social Theory*. SAGE Publications.

Siwicki, B. *Global Edition Connected Health How remote patient monitoring is moving into the mainstream.* Healthcare IT News. https://www.healthcareitnews.com/news/how-remote-patient-monitoring-moving-mainstream

Smet, M. (2002). Cost characteristics of hospitals. *Social Science & Medicine. 55(6)*. DOI: 10.1016/s0277-9536(01)00237-4

Statchel, R., & DeLaHaye, M. (2015). Security Breaches in Healthcare Data: An Application of The Actor Network Theory. *Issues in Information Systems. 16(2)*. https://pdfs.semanticscholar.org/41f8/91e32be7b3b4e4f4002139554581518daaa3.pdf

Sullivan, M. (2020, May 11). *Telehealth is driving a boom in digital communications.* Healthcare Finance. https://www.healthcarefinancenews.com/news/telehealth-driving-boom-digital-communications

Telemedicine and data exploitation. (2021, October 28). Privacy International. https://privacyinternational.org/

theDataMap. (2013). Harvard University, Institute for Quantitative Social Science (IQSS), Data Privacy Lab. http://www.thedatamap.org

Bertonici, M. & Jackson, V.. (2019, July 31). *Is Your Patient Portal Secure? Study Shows Healthcare Organizations' Traditional Cybersecurity Measures are Insufficient Against Today's Attacks.* The National Law Review. https://www.natlawreview.com/article/your-patient-portal-secure-study-shows-healthcare-organizations-traditional

Torrence, R. (2021, October 20). *Security flaws in health apps, APIs potentially put millions of patient records at risk, report finds.* Fierce Healthcare. https://www.fiercehealthcare.com/tech/report-shows-patient-data-vulnerable-to-hacks-third-party-aggregators

Wang, Y., Tran, P., & Wojtusiak, J. (2022). From Wearable Device to OpenEMR: 5G Edge Centered Telemedicine and Decision Support System. *In Proceedings of the 15th International Joint Conference on Biomedical Engineering Systems and Technologies. 5.*

Yetisen A., Martinez-Hurtado J., Ünal B., Khademhosseini A., & Butt H. (2018). Wearables in Medicine. *Advanced Materials (Deerfield Beach, Fla.)*. DOI: 10.1002/adma.201706910.

2020 Healthcare Data Breach Report: 25% Increase in Breaches in 2020. (2021, January 19). HIPAA Journal. https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/#:~:text=According%20to%20Emsisoft%2C%20at%20least,and%202.69%25%20of%20breached%20records.

33 vulnerabilities found in the data transfer protocol for wearable medical devices. (2022, February 1). Kaspersky. https://usa.kaspersky.com/about/press-releases/2022_33-vulnerabilities-found-in-the-data-transfer-protocol-for-wearable-medical-devices