Modernizing The Health Insurance Portability and Accountability Act

Tucker Lehman

Public Policy Incubator

May 9, 2023

Table of Contents

Executive Summary

This paper will go over one of the main problems that concern healthcare facilities today, and that problem would be hacking. It will prove that there have been many hacking incidents over the past few years, and each of these incidents have cost the concerned facilities thousands upon millions of dollars. There will be more detail in the paper, but the two main ways that these healthcare facilities are getting hacked are by actual breaches of security, and phishing emails. Both of these breach security, but the former breaches it through means of an actual weak security system, and the latter is breached through the negligence of those opening the emails and falling for the scam.

Then the paper will go over the solution to the problem. This solution will be to update the HIPAA Security Rule to account for our modern times, by updating the security and increasing training for all affected healthcare facilities. The way that these healthcare facilities would be chosen for this change would be through the already existing and previously stated rule, which says that all healthcare facilities transmit data electronically, which is perfect since the entire solution in this plan is to protect electronic data. However, some healthcare facilities may not be able to afford the changes, due to their size, so it would be unwise to put too many changes and additions on them in their budget. This is why the solution will be an evolving one, which essentially means that those who can't do as much, will only have to meet a minimum requirement, while those who can do more will meet a higher standard.

These differences will be chosen through patient records. It is a simple and easy solution to be able to tell how big a healthcare facility is, and how much they could afford. Those patient records are already tracked, which means that there won't be a need to go out of the way to track the information all down. Then, after the primary changes are all made between each facility, every few years, those who were allowed to not make as many changes will slowly have to add

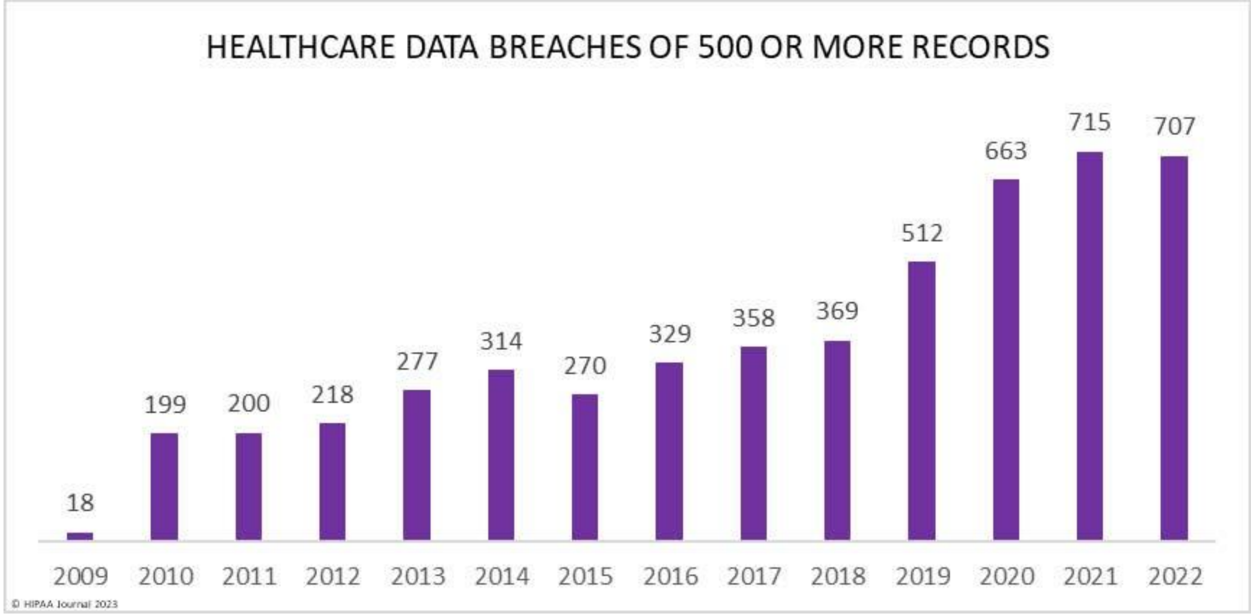
more and more of the other ones over time. This is where the benefit of the plan comes in, as it allows the smaller healthcare facilities to not be under so much pressure, while still increasing their security to greatly reduce incidents. The other benefits, aside from fixing a problem that has been plaguing healthcare facilities for years, is also that since this solution is based off of a previous plan, there won't be too much extra work in implementation.

This means that the budget, the enforcement, and every other legislation detail that isn't new, will already be taken care of due to the previously existing rule. Not only that, but the improvement that will be seen from the implementation of this plan will be astounding. This paper will show quotes and statistics for problems and how they greatly increase hacking incidents, such as phishing emails. Then this paper will show quotes on other professionals talking about how adding our solutions will greatly reduce those increased incidents. This means that the hacking incidents will greatly decrease, patient's private information will be secured, and the solutions are simple enough that it will not take too much effort to put them into place.

As stated before, and as what will be stated shortly, these hacking incidents are a serious problem. They put patient's data and information at risk, which can lead to identity theft, they cost hospitals and other healthcare facilities millions of dollars for each instance, and currently, no one really knows what to do to effectively and quickly solve the problem. This is why our solution is so important, since it fixes all of those problems, while also not needing a lot of work to get done.

The Problem

Firstly, the most important thing to talk about before the solution is the problem. This portion of the paper will go over all of the data proving that there is a serious problem in the healthcare industry. That problem is the rampant amount of hacking that these healthcare facilities have to go through.



Data chart from HIPAA Journal

This chart shows that over the past thirteen years, the number of large breaches, 500 records or more, maintained an erratic increase year-to-year. Now if the data was only showing 500 records that were exactly compromised, it will still show 35,750 records in 2021. To explain how important this is, the compromised records are protected health information or PHI. These records are akin to bags of money stolen in a bank heist. PHI includes full name, images, physical address(es), email address(es), phone number(s), IP address(es), account number(s), and social security number, among other things which shows how important these records could be to the individual, all according to US Department of Health and Human Services.

And, once again, the number is growing, and will continue to. There will be the occasional low year, but the number of people made vulnerable will keep increasing. Furthermore, this chart does not tell the entire story due to its limits: it only records large data breaches of at least five hundred compromised records. It is not recording the smaller ones, and there are a vast number of smaller ones: 48% of executives in smaller hospitals confirm that they had to shut down the organization between September 2022 and February 2023, and as of 2021, 89% of healthcare organizations reported an average of forty-three ransomware attacks a year. That is one attack every eight and half days, and approximately three and a half attacks every month. For a flat number of people whose data was compromised, in 2021, there were around 44.9 million victims or to put it in perspective that is about twice the population of New York.

Next, let us look at average costs. It can be assumed that data breaches lead to a large loss of capital, but the actual numbers are striking, to say the least. According to the HIPAA Journal In 2022, the average cost of a healthcare breach was ~$10.1 million. This is almost a 10% increase from 2021, and a little over a 40% increase from 2020.To do the math, with a total cost of ~$10.1 and a total target count of ~44.9 million, that comes out at about ~$0.22/record. That does not seem like much, but only 5 compromised records already cost $1.10 on average, and that adds up incredibly quickly, especially considering that, in 2021, the average breach exposed ~3.32 million records, meaning that the average breach in 2021 cost ~$748,815.14.

For a point of comparison, according to NBC 5, the median price of a house in the Chicago Metropolitan Area at the time was ~$310,000 which is a little less than half of the average 2021 cost. Imagine having to pay for two Chicago Metro Area houses about every 8.5

days. What makes this more dangerous is that, while a large medical facility has much more money than the average individual buying a house in the Chicago Metro Area, a small or medium-sized hospital could be drained dry easily. It has made worse when compounded with the fact that, due to a lack of money, smaller facilities are far easier to break into, leading to a situation that could very easily drive the hospital to bankruptcy.

On a very dark, but incredibly important note, looking at disruptions to functionality is also incredibly important. On the side of stolen PHI, according to Tausight, 95% of identity theft was committed using information gained from a medical data breach. We do not need to restate the kind of chaos that identity theft can cause. That 95% needs to be dashed, and it needs to be dashed sooner rather than later. On the more morbid side, 20% of affected hospitals reported increased patient mortality. Of that 20%, 57% reported worse outcomes for patients that did survive, and 50% reported an increase in medical complications.

This is unacceptable. Medical facilities are places where the slightest problem, the slightest disruption, can result in death. To draw a last point with this morbid topic, allow us to tell you of something that happened in October in 2022. The second-largest nonprofit hospital chain in the United States, boasting 140 hospitals and more than 1,000 care sites across 21 states, was hit by a massive ransomware attack. The results? Rescheduled appointments, diverted ambulances, and in Washington state, the delaying of critical procedures, including a CT scan to check up on a brain bleed. Unsurprisingly, brain bleeds are incredibly dangerous, with a five-year survival rate of ~26.7%, and that includes treatment. A delay of even a few weeks, which is likely what happened here, could highly likely be fatal according to Medicine Net. To sum it all up, the hacking of medical systems is incredibly dangerous in numerous diverse ways, which is why this must be remedied immediately.

Over thirteen years, HIPAA journal has reported 5,150 healthcare data breaches, with over 382,262,109 healthcare records being exposed. These data breaches occur due to many reasons such as human errors, technology failures, and cyber-attacks. There is no one way to protect against human error. However, it can be suggested to perform yearly audits on processes. Technology failures are a key issue in healthcare organizations. Many hospitals store data with onsite servers and/or cloud base services. This is concerning because according to the software protection company Malwarebytes, one in six companies that store data in the cloud has experienced a data breach. Having outdated or poorly maintained IT systems creates more susceptibility to data breaches. With a compromised IT system, cyber-attacks will happen in only a matter of time. Cyber-attacks are caused by external hackers who use various techniques to gain access to patient data. The increasing amount of patient medical data being stored and shared online has also created more opportunities for data breaches. This is extremely dangerous because there are several consequences of data breaches: identity theft, financial fraud, and reputational damages to healthcare organizations

Medical data storage has been constantly evolving with advancements in technology and increased concern for data security and privacy. Traditionally, hospitals have stored patient data on paper, which was time-consuming and difficult to manage. This also made it difficult to share information with other healthcare providers. With recent technological advancements, medical data is currently stored online. EHRs or electronic health records are kept on a cloud service or an onsite server. These services must comply with the Health Insurance Portability and Accountability Act (HIPAA), a federal law enacted in 1996 to protect the privacy and security of personal health information. HIPAA sets national standards for the protection of sensitive health information, known as Protected Health Information (PHI), which includes any identifiable information related to an individual's past, present, or future health condition. To be HIPAA compliant, cloud storage must offer two-step authentication or an encrypted single sign-on. Encryption is the process of converting sensitive data into an unreadable format, which can only be accessed by authorized personnel. With encrypted data, data backup and recovery must be an option. This ensures that patient data is not lost in the case of a cyber-attack or natural disaster.

Personal Medical data has become a target for hackers due to the increased value of personal data. Hackers are trying to obtain any information, but names, birth dates, social security numbers, and medical history have a high price tag. Additionally, medical data is useful for targeting individuals based on HIPAA-protected information.

To know what is wrong with using “cloud servers,” one needs to understand what the cloud is and the main types of cloud. Contrary to widespread belief, the cloud is physical and tangible, as it refers to the servers that store data. The three distinct types of cloud are Public cloud, Private cloud, and Hybrid cloud. A private cloud is a cloud that is used internally in a company. However, a public cloud is used in public spaces, such as delivery services. Lastly, a hybrid cloud is a mix of the two.

According to cloudwards.net, there will be over 100 zettabytes of data stored in the cloud by 2025. Leftronic.com reports that around 90% of companies use some type of cloud service, with around 80% of those enterprises using Amazon Web Services as their primary cloud platform. Acropolium.com says that 98% of healthcare organizations have either planned to adopt cloud computing or have already adopted it. This shows that cloud usage is incredibly important to most companies and organizations in the world, especially in the U.S.

Because it is so prevalent in modern times, it leads one to believe that the cloud is a system with limited flaws and many benefits. While there are benefits to using cloud servers, there are also some major drawbacks. For example, according to Knowledgehut.com and Insights.edu, one of the main problems with cloud servers is their data security. This is because of many reasons, such as lack of visibility and control tools, Cloud misconfiguration, and neglect in cloud data management. However, this is not the only problem with the clouds. There is also a high dependency on the network and a lack of flexibility regarding moving applications between multiple cloud systems.

Medical organizations house a lot of confidential data, so the need for data protection has increased drastically in this industry. Therefore, it was a problem in 2021 when over 715 data breaches occurred in the United States (Hipaajournal.com). It did not get better in 2021 as there were a reported 707 data breaches. To put it into perspective, instead of 54 million records being breached and hacked from healthcare data systems in 2021, there were only 51.9 million records in 2022 instead. According to techjury.net, each of those incidents in 2021 cost businesses an average of 9.3 million dollars per incident.

However, this is not just affecting the companies, it is also affecting the customers and consumers. One incident of data breaching happened in 2022, when OneTouchPoint's data was breached, affecting more than 4.1 million individuals (cheifhealthcareexecutive.com). In the same year, Advocate Aurora Health's data was breached, affecting over 3 million patients (about the population of Arkansas). It is important to note that approximately 95% of identity theft comes from stolen healthcare records (techjury.net), and since healthcare has the highest number of security breaches, it is an increasing problem.

Medical data is incredibly important and sensitive. Third parties gaining access to medical data can be (and is) used for many undesirable outcomes. There have been reports in the wake of Roe v Wade's overturning of states that have outlawed abortion buying data from women's health applications and websites. This is to avoid it being used for many purposes, such as anti-abortion advertising and using the information to prosecute women for terminating their pregnancies.

For instance, a few years ago, Facebook was caught "...[having] created a machine-learning system to help detect sensitive health data and blocked data that contained any of 70,000 health-related terms…[investigations] have found Facebook's code on the websites of hundreds of anti-abortion clinics…[and the investigators] analyzed the sites of nearly 2,500 crisis pregnancy centers—with data provided by the University of Georgia—and found that at least 294 shared visitor information with Facebook. In many cases, the information was extremely sensitive—for example, whether a person was considering abortion or looking to get a pregnancy test or emergency contraceptives." In plain language, this means that Facebook sold personal information that should have been private to corporations and religious organizations looking to prevent people from going through abortions. Whether or not one supports abortion, this is a massive invasion of privacy and should not be allowed to freely continue.

There have also been instances of companies buying data from websites and hackers of individuals with certain disorders to know who best to market to. Recently, a research project from Duke University involved fictitiously attempting to buy mental health data to see what the general atmosphere of such data brokerage was like. To their surprise, the article notes "... [the study] consisted of asking 37 data brokers for bulk data on people's mental health. Eleven of them agreed to sell information that identified people by issues, including depression, anxiety, and bipolar disorder, and often sorted them by demographic information such as age, race, credit score, and location…Some of the brokers were particularly cavalier with sensitive data. One made no demands on how the information it sold was used and advertised that it could offer names and addresses of people with “depression, bipolar disorder, anxiety issues, panic disorder, cancer, post-traumatic stress disorder, obsessive-compulsive disorder, and personality disorder, as well as individuals who have had strokes and data on their races and ethnicities” ...”

This is another breach of consent, as an individual does not expect their confidential medical data to be sold to companies for targeted advertising. This invasion of privacy is completely needless, as there is no need for strangers to know an individual’s private diagnosis without due cause.

Hacking medical devices is also a considerable problem because data could be (and is) stolen, which could lead to catastrophic consequences. In 2022, The FBI had to step in to prevent a cyberattack on Boston Children’s Hospital from Iran. Unfortunately, this was not the first time. A few years before, a man hacked into and damaged the medical facility’s computers, which “...cost the facilities tens of thousands of dollars and disrupted operations for days.”

Due to the breaches in data and disrupted operations in a hospital, people could have died, and many more could now have the security of their data compromised. This kind of issue can easily affect anyone receiving intensive medical care.

Although one may say “I’m not in any of these categories, so I’m safe,” these are simply examples. The underlying point is the immoral tracking, use, and distribution of sensitive data. If it happens to entire hospitals, let alone people seeking abortions and suffering from mental conditions, it can happen to anyone. With increasing technological advancements, this problem is urgent and will continue to grow. In conclusion, the brokerage of medical data is a grave issue and is teeming with opportunities for disaster. Most people do not know that their information is exposed, and brokers are often not careful enough with the vital information that they hold. Also, there is currently no legislation clarifying what is and is not allowed in terms of buying and selling such data. As such, finding a solution to this problem is of utmost importance.

There were a lot of hacking incidents over the last few years that show that there should be a new change when it comes to how we treat healthcare cybersecurity. According to Touro University, healthcare facilities lost around 20 billion dollars (about $62 per person in the US) due to ransomware attacks in just 2020 alone, and the number did not improve much in the following years. These number figures came from the impacted revenue, ransom paid out, and lawsuits that came from these hacking incidents and the numbers rise when specific healthcare facilities are targeted. For example, according to Touro University, Marene Allison, Johnson & Johnson's chief information security officer, said that Johnson & Johnson experiences 15.5 billion cybersecurity incidents daily when the article was published.

However, while you can prove that millions of dollars are being lost every year to hacking and ransomware incidents against healthcare facilities, the question is whether most healthcare facilities face this problem? Also, aside from money, are there any other negatives that come from healthcare hacking? The answer to both questions is yes, and brookings.edu helps answer the first one. According to Brookings, the 2020 HIMSS Cybersecurity Survey showed that 70% of hospitals surveyed reported a significant security incident. Also, according to Forbes, cyberattacks increased by 71% towards healthcare facilities and hospitals, with that number only increasing.

Now for the last question, are there other harms that come from these hacking incidents? According to Reuters, more than 70% of healthcare hacking incidents that occur help fuel identity theft, which is on a completely different spectrum when it comes to the amount of damage that it can cause and how many other crimes it can lead to. All these problems show that there should be a fix, as these problems are persisting, and they persist for most healthcare facilities, which proves it is a national issue.

Personal data is any information that can be used to identify an individual. In the black markets today, personal data is a highly valuable commodity that is bought and sold by numerous companies for several reasons. However, not all personal data can be sold due to certain limitations and regulations that are in place from the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States. Under the GDPR, third-party agencies can sell personal data if there is consent from the data subject. Consent is typically given when accepting a required terms and condition. GDPR does not make data selling illegal or difficult to do. However, CCPA has created more protections for personal data. In the state of California, users whose data is being collected must have an option to opt out. This is a great first step because the people who care about their personal data can opt out. Also, under the CCPA, it is illegal to sell any personal data if the subject is under 16 years old. This is alarming because there should be more protection for minors.

With limited protection under the GDPR and CCPA, personal data such as addresses, email addresses, telephone numbers, locations, and demographic information. With the protection of HIPAA, Health Insurance Portability and Accountability Act, health records or financial information cannot be sold without explicit consent from the individual. With the protection of HIPAA, why are there constant data breaches at healthcare facilities? Hackers are hacking into vulnerable systems to obtain public personal data. All healthcare facilities collect legal names, addresses, emails, and phone numbers. This information is only protected by HIPAA if it is in medical documents.

The Solution

This concrete plan would be a new (updated) policy law that would create a national standard for all healthcare and hospital facilities concerning their cybersecurity. We already went over an extensive study on how there is a problem, so now that we have proven that it is a national issue, what would be the best way to implement a national standard? Well as it turns out, there is already a national law that applies to all healthcare facilities that transmit any personal data online. This is from the US Department of Health and Human Services and the law is known as the HIPAA (Health Insurance Portability and Accountability Act) Security rule. This law was put in place in 2003 and was essential during its time because documents were starting to go from paper to electronic, which meant that a new law would have to be put in place. This law applies to all healthcare facilities that transmit any personal individual data online as stated before, so it already covers all the healthcare facilities that we would need them to. The rule also permits that those documents are not disclosed to any third party. In fact, the entire skeleton of a law that you would need is right there, including previous parameters for who is covered, slight enforcement policies, plans for required updates, budget, and agencies in charge of protecting it. Those agencies are The Department of Health and Human Services, and the Office for Civil Rights.

So, the natural question that would be asked is, if the law already has a lot of what we need, why do we need to spend more potential to update it? Well, the issue comes from how old the law is, and how much technology has adapted and improved since then. It has already been proven, and it is already extremely clear that there is a problem with the protection for hospitals. This is because while technology has improved, which has given us a lot of momentous changes, its improvement has also made it easier for hospital records to be hacked and taken. So, the question is, what would we have to do to make this HIPAA Security Rule strong enough to survive in this modern time? The answer is, increased enforcement, and adding more required changes for all healthcare facilities. Firstly, let us address the changes that would be made.

A lot of these changes come from HealthCare Dive. Firstly, security checks every two weeks that would make sure that there are no active holes in their security. Secondly, A multi-factor authentication system so that there is not only one way to access any of the personalized data. This change was backed up by the White House and by AHA (American Heart Association) who said changing passwords often was an essential idea. Thirdly, reducing the need for human error by continually adding more security and upgrading whenever possible. This change is supported by Brad Parks, chief product and marketing officer at Morpheus Data, a cloud management platform company.

Fourthly, separating more critical systems from general systems, so that all the data is not stored in one warehouse, and if there is a hacking incident, none of the more critical data would get stolen. This idea was backed up by resilience Insurance Chief Risk Officer Richard Seiersen, a former general manager of cybersecurity and privacy for GE Healthcare. Fifthly, employing intrusion detection software to stop phishing emails or other malware attacks. This change is supported by John Riggi, an FBI veteran and senior adviser for cybersecurity and risk at the American Hospital Association. Finally, the last change would be empowering and training the staff to be able to spot and more easily detect breaches or phishing emails. This is because more than 90% of successful cyberattacks start with a phishing email, supported by the Cybersecurity and Infrastructure Security Agency, or CISA.

There are two obvious problems and questions with this plan. The first is, how would a healthcare facility know how many changes to implement, and what happens if they cannot afford it? The first answer to that question is patient records. The number of patient records that a healthcare facility has is already used to differentiate it from another smaller healthcare facility. In some places, including places that are more rural in nature, or that receive less patients, will have a more challenging time trying to implement all these changes, which is also where the second question comes in. This is why this national plan will be a tiered system, including different changes for each area depending on the location and amount of patient records for each facility.

This tiered system would require a baseline change across the board, which would be training the staff to better handle and detect phishing email scams, consistently upgrading their security systems, and having a multi-factored system. These would be the very baseline of changes, as these have had most research backed up on them, suggesting that each of these individual changes would reduce the chance of getting hacked. Then, depending on the amount of patient records a facility has, they will have to add more of the other changes on top of the baseline changes, as they might already have the baseline changes already considering their size. The idea of the baseline changes is so that smaller facilities have a rubric of standard so that they can be protected, and so that bigger facilities have an idea of what should already be strengthened.

Then the tiered system would take a similar page out of HIPAA's time rule, as they made it so smaller facilities would not have to add all the different changes right away, but as the years went on, they would have to adapt increasingly to the required changes over time. This means that while the bigger facilities would already have to adapt more of the changes early on, the smaller facilities would not be left behind, but forcing them to change as quickly as the rest would only harm them instead of benefiting them. To sum up the plan so far, it would be a tiered system that affects different healthcare facilities depending on the size of them. This “size” would be determined by the amount of patient records that each of the facilities have, and this would be spearheaded by HIPAA itself, as they already know this information, and the two previous agencies listed that oversee enforcing this rule.

Then, according to the number of patient records a facility has, they would be forced to adapt more or less of the required changes as listed before. However, regardless of size, every single facility would be forced to meet three of the most important requirements, being training employees to detect phishing scams, having a multi-factored system, and having constant updates to their security systems to stay up to date. Then, over time, each of the smaller facilities that could only meet the required changes would have to adapt to the other changes bit by bit, effectively keeping every single facility up to date and protected by the time it is all over.

There is also one more piece to the plan, which is the enforcement. To put it simply, some healthcare facilities might have the ability to add on more changes, even if they are put into the category of just having to meet the baseline. Not only that, but others may also just want to add on more changes in general. For those who would do that, an incentive program would be put into place, which would reward those for going above and beyond. Whether those benefits be tax cuts, extra funding, or whatever else, these benefits would be an incentive to make these facilities try and update their systems faster, and with less complaints. However, there may be those who do not enact the changes that they should, when they should. In which case, punishments would be enacted, which would be the opposite of the benefits of the incentive program. The incentive program, the negative punishment would also be protected by the agencies listed before, including HIPAA, The Department of Health and Human Services, and the Office for Civil Rights. Not to mention, this would only be increased enforcement, as the enforcement that already existed with the previous HIPAA Security Rule would still be in place.

Final Thoughts, The Benefits

Now it is on to the final part of the paper, which explains the benefits of this plan, and why it is better than other plans. One of the biggest reasons why this plan would be so valuable is because the work is already half done. Simply put, the fact that the skeleton of the plan is based on the HIPAA Security Rule makes it much easier for legislation and healthcare facilities themselves. For starters, it is a good plan for legislation because even though there are some new things to implement, such as adding baseline changes, and the reward system, there will not be as much work or laws to push as with a completely new law. If nothing else, this is a modernized version of the previous existing law. Not only that, but this plan is also cost effective. Of course, money will be spent, but compared to having to pull the money from another program, or somewhere else, the money and budget for it already exists. I

This idea is not simply good for legislation however, it is also good for the healthcare facilities themselves. The first reason that this is good for them is because it provides a quick and easy solution to a problem that has been affecting them for years. They are losing millions of dollars each hacking incident, and they are also losing the faith of their patients. So, by either adding on a few changes, or if they already have the changes made, simply making sure they are up to date consistently, they get to regain the trust of their patients while putting an effective end to incidents that cost them millions. To go further on that note, since they are already losing so much money with these incidents, spending less money on a solution, albeit still money, makes more business sense than simply hoping that a hacking incident does not happen to you.

It is also a promising idea for the healthcare facilities in rural areas, as they will not be forced to spend too much money to adopt all the changes right away. In fact, the very idea that each healthcare facility is judged off the patient records that they have, instead of being forced into regional areas, is a big plus for them. It makes everyone feel as if they are gaining something with this plan, instead of someone having to sacrifice something so that the plan will work. Legislation does not have to sacrifice much, big healthcare facilities do not have to sacrifice much, and smaller more rural facilities do not have to sacrifice much either. And even with that non-sacrifice, everyone wins. Legislation gets praised for spearheading a cost effective solution quickly, and the healthcare facilities get less hacking and more protection for the long term. It is an effective win-win-win scenario for every single party involved, except for the hacking party, which is exactly how our hospitals and healthcare facilities should feel.

Works Cited

A Cost Analysis of Healthcare Sector Data Breaches Health Sector Cybersecurity Coordination Center (HC3) HC3@HHS.GOV `` Executive Summary. 2019.

"Chicago Housing Market: Prices | Trends | Forecast 2021-2022." *Redwood Construction Group*, redwoodbuilt.com/blog/chicago-housing-market-prices-trends-forecast-2021-2022. Accessed 9 Apr. 2023.

---. "IBM: Average Cost of a Healthcare Data Breach Reaches Record High of $10.1 Million." *HIPAA Journal*, 28 July 2022, www.hipaajournal.com/ibm-2022-cost-of-a-data-breach-healthcare-10-million/.

Stringfellow, Angela. "Healthcare and Cybersecurity: 35 Key Statistics and Facts You Should Know." *Tausight*, 1 Nov. 2022, www.tausight.com/healthcare-and-cybersecurity-key-statistics/#:~:text=The%20average%20cost%20of%20a. Accessed 9 Apr. 2023.

"What Are the Chances of Surviving Bleeding in the Brain?" *MedicineNet*, www.medicinenet.com/chances_of_surviving_bleeding_in_the_brain/article.htm. Accessed 9 Apr. 2023.

Witts, Joel. "Healthcare Cyber Attack Statistics 2022: 25 Alarming Data Breaches You Should Know." *Expert Insights*, 1 Apr. 2022, expertinsights.com/insights/healthcare-cyber-attack-statistics/.

"28 Captivating Cloud Computing Statistics." *Leftronic.com*, leftronic.com/blog/cloud-computing-statistics/.

"A Researcher Tried to Buy Mental Health Data. It Was Surprisingly Easy." *NBC News*, www.nbcnews.com/tech/security/researcher-tried-buy-mental-health-data-was-surprisingly-easy-rcna70071.

“Cloud Computing in Healthcare Explained [Use Cases Included].” *Acropolium.com*, acropolium.com/blog/cloud-computing-healthcare/#:~:text=A%20staggering%2098%25%20of%20healthcare. Accessed 9 Mar. 2023.

Cozens, Bill. “Cloud Data Breaches: 4 Biggest Threats to Cloud Storage Security.” *Malwarebytes*, www.malwarebytes.com/blog/business/2022/06/cloud-data-breaches-4-biggest-threats-to-cloud-storage-security.

“FBI Blocked Planned Cyberattack on Children’s Hospital, Director Says.” *NBC News*, www.nbcnews.com/tech/security/fbi-blocked-planned-cyberattack-childrens-hospital-director-says-rcna31456.

Journal, HIPAA. “2022 Healthcare Data Breach Report.” *HIPAA Journal*, 24 Jan. 2023, www.hipaajournal.com/2022-healthcare-data-breach-report/#:~:text=There%20were%2011%20reported%20healthcare.

Morrow, Timothy. “12 Risks, Threats, & Vulnerabilities in Moving to the Cloud.” *SEI Blog*, 5 Mar. 2018, insights.sei.cmu.edu/blog/12-risks-threats-vulnerabilities-in-moving-to-the-cloud/.

“Most Popular HIPAA-Compliant Cloud Storage Services.” *Https://Blog.netwrix.com/*, blog.netwrix.com/2020/08/13/hipaa-compliant-cloud-storage/#:~:text=A%20HIPAA%2Dcompliant%20cloud%20storage%20must%20offer%20two%2Dstep%20authentication. Accessed 9 Mar. 2023.

Oldham, Grace, and Dhruv Mehrotra. “Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients – the Markup.” *Themarkup.org*, themarkup.org/pixel-hunt/2022/06/15/facebook-and-anti-abortion-clinics-are-collecting-highly-sensitive-info-on-would-be-patients. Accessed 9 Mar. 2023.

Sumina, Vladimir. “26 Cloud Computing Statistics, Facts & Trends for 2021.” *Cloudwards*, 22 July 2021, www.cloudwards.net/cloud-computing-statistics/.

“The 11 Biggest Health Data Breaches in 2022.” *Chief Healthcare Executive*, www.chiefhealthcareexecutive.com/view/the-11-biggest-health-data-breaches-in-2022.

“Top 15 Cloud Computing Challenges [with Solution].” *Www.knowledgehut.com*, www.knowledgehut.com/blog/cloud-computing/cloud-computing-challenges.

Touro College Illinois. “The 10 Biggest Ransomware Attacks of 2021.” *Illinois.touro.edu*, 12 Nov. 2021, illinois.touro.edu/news/the-10-biggest-ransomware-attacks-of-2021.php. The 10 Biggest Ransomware Attacks of 2021 | Touro College Illinois

West, Emily Skahill and Darrell M. “Why Hospitals and Healthcare Organizations Need to Take Cybersecurity More Seriously.” *Brookings*, 9 Aug. 2021, www.brookings.edu/blog/techtank/2021/08/09/why-hospitals-and-healthcare-organizations-need-to-take-cybersecurity-more-seriously/.

Brooks, Chuck. “Cybersecurity in 2022 – a Fresh Look at Some Very Alarming Stats.” *Forbes*, www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=47c37ea36b61. Accessed 9 Mar. 2023.

“Healthcare Data Hacking Could Lead to Identity Thefts.” *Reuters*, 23 Sept. 2019, www.reuters.com/article/us-health-privacy-cyber-idUSKBN1W82K3. Accessed 9 Mar. 2023.

U.S. Department of Health & Human Services. “Summary of the HIPAA Security Rule.” *HHS.gov*, 19 Oct. 2022, www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

“8 Ways Hospitals Can Prevent a Cyberattack.” *Healthcare Dive*, www.healthcaredive.com/news/hospital-cyberattack-prevention-commonspirit-hack-breach/635407/#:~:text=8%20ways%20hospitals%20can%20prevent%20a%20cyberattack%201. Accessed 9 Mar. 2023.

Gsimon. “Electronic Medical Records: The Components of a Medical Record.” *American Retrieval Company*, 16 Aug. 2021, https://americanretrieval.com/medical-record-components/.

"Healthcare Cyber Attack Statistics 2022: 25 Alarming Data Breaches You Should Know." *Expert Insights*, 24 Nov. 2022, https://expertinsights.com/insights/healthcare-cyber-attack-statistics/.

"Healthcare Data Breaches Due to Phishing." *HIPAA Journal*, https://www.hipaajournal.com/healthcare-data-breaches-due-to-phishing/.

Stringfellow, Angela. "Healthcare and Cybersecurity: 35 Key Statistics and Facts You Should Know." *Tausight*, 3 Nov. 2022, https://www.tausight.com/healthcare-and-cybersecurity-key-statistics/#:~:text=The%20average%20cost%20of%20a,highest%20cost%20of%20any%20industry.

Stringfellow, Angela. "Healthcare and Cybersecurity: 35 Key Statistics and Facts You Should Know." *Tausight*

Starks, Tim, and McKenzie Beard. "Analysis | an 'Unprecedented' Hospital System Hack Disrupts Health-Care Services." *The Washington Post*, WP Company, 6 Oct. 2022, https://www.washingtonpost.com/politics/2022/10/06/an-unprecedented-hospital-system-hack-disrupts-health-care-services/.

"Emergency Surgery." *MaineHealth*, https://www.mainehealth.org/Services/Surgery/Emergency-Surgery.

Davies, Aran. "System Security Software - How Much Time Does It Take to Create One?" *DevTeam.Space*, 13 July 2022, https://www.devteam.space/blog/how-much-time-does-it-take-to-create-a-security-software-solution/

"Biggest Cyber Threats in Healthcare (Updated for 2023): Upguard." *RSS*, https://www.upguard.com/blog/biggest-cyber-threats-in-healthcare.

"Cybersecurity Career Pathway." *Cyberseek*, https://www.cyberseek.org/pathway.html.

Uche, Nneoma. "What Is a Typical Cybersecurity Salary?" *Forbes*, Forbes Magazine, 16 Feb. 2023, https://www.forbes.com/advisor/education/cyber-security-salary-outlook/#:~:text=Cybersecurity%20salaries%20may%20also%20vary,make%20a%20six%2Dfigure%20income.

Bai, Ge, and Hossein Zare. "Hospital Cost Structure and the Implications on Cost Management during COVID-19." *Journal of General Internal Medicine*, U.S. National Library of Medicine, Sept. 2020, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7326305/.