Patient Privacy Exposed: A Closer Look at HIPAA in the Context of a Pandemic

Richa Upadhyay
Stanford University

Abstract

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is strict legislation executed to protect patient data and privacy. With five titles outlining healthcare information ranging from health insurance coverage to electronic health care, HIPAA is responsible for the national standards for disclosure, consent, and protection of health information (CDC, 2018). During the COVID-19 pandemic, HIPAA has come to the forefront of conversation among healthcare and policy professionals as a result of the transition to recording patient data online and the commonality of noncompliance. However, in recent months, there has been a push for more leniency to allow for more comprehensive research to be conducted on COVID-19 despite the large number of privacy breaches and the compromise on the purpose of HIPAA. The pandemic, a seemingly temporary climate, demands research by scientists to track benefits of emergency-implemented strategies and physician-patient appointments to be held virtually; on the other hand, current HIPAA presents challenges by requiring anonymity and certain conditions to be met with regards to telehealth. By exploring recent modifications to HIPAA legislation made by the Department of Health and Human Services and the Office for Civil Rights and its downfalls in maintaining confidentiality, this paper will focus on how HIPAA should redefine what privacy is to benefit both patients and researchers during the pandemic. This paper will also investigate how HIPAA should be implemented to protect patient privacy when treating COVID-19 patients and introduce considerations when redesigning HIPAA after examining the model employed by Taiwan and Singapore. This research will provide details on a better balance of HIPAA between privacy protection and publicizing data during emergency situations by breaking down each of the major waivers.

Introduction

Healthcare, among other social and political shifts, was prioritized during the COVID-19 pandemic. According to the New York Times's case

tracking, COVID-19, as of March 28, has accumulated to a total of 30.3 million cases in the United States (The New York Times, 2021). As a result of the pandemic, many companies have transitioned to an online working space, and similarly, individuals have navigated ways to be productive remotely. Healthcare providers and hospitals are no exception as telehealth has become more popular in the past months. Changes in health policy have come to the forefront of conversation among health-related fields, specifically in regard to how well patient information is being protected at a time where case numbers and hospital statistics are being published and updated on news channels and government websites. And additionally, concerns about how effective past legislation about patient privacy is at adapting to current changes in healthcare are provoked.

When discussing patient privacy, HIPAA is never too far away from the conversation. The Health Insurance Portability and Accountability Act (HIPAA) was created in 1996 and incentivized the use of digitized records to guard Protected Health Information (PHI) productively (Lenert, 2020). It strives to protect consumer's rights, emphasize the focus on health privacy, and improve quality of care (Herold, 2015). As a result of the pandemic and the transition to telehealth, the Department of Health and Human Services (HHS) and the Office for Civil Rights (OCR) have issued a few lenient provisions towards HIPAA. This modified legislation allows scientists to investigate patient data and examine the benefits of implemented strategies, but unintentionally compromises patient privacy. After reading scholarship written by medical and privacy professionals on the breakdown of the HIPAA waivers, gaps in technology systems, and comparing America's model to other countries, the government should have modified HIPAA to include a better balance between privacy protection and publicizing data to advance COVID-19 research.

Although these HIPAA waivers are necessary to advance research and treatment for the coronavirus, the lack of specificity in the waivers has contributed to an *unnecessary* exposure to patient privacy, which can lead to a range of harmful consequences including private health data being published on the internet. The importance and relevance of this topic is clear; Americans value privacy deeply, and when that is challenged, it is imperative to find resolutions. This research paper will scrutinize the four major HIPAA waivers passed by the HHS and OCR, arguing that these waivers—especially the language used—have created far too many gaps that can expose patient privacy. First, the March 13th waiver, specifically its vague language and one-size-fits-all approach to emergencies, is examined. Next, the telehealth waiver is discussed with a closer look at the undermining technology platforms used. Then, the pros and cons of the business associates and community-based testing sites waivers, attempting to define its qualifier, "good faith," is analyzed. The paper goes on to compare government intervention methods employed in Taiwan and Singapore—countries with a lower number of COVID cases—to propose

possible solutions for America. And lastly, considerations are presented for looking forward in a post-pandemic society.

Benefits of the HIPAA Waivers

Many professionals in health policy, healthcare, and research believe that it was necessary for HIPAA to be adjusted quickly to accommodate the shift to telehealth. Recent HIPAA waivers have allowed more patients to be treated via screens, while also decreasing the amount of in-person contact. Rajiv Levanthal, the managing editor at Healthcare Innovation known for his work on healthcare information technology, notes that with these waivers, healthcare providers are able to share patient data faster and easier. These waivers also allow physicians to share data outside of their healthcare system (Leventhal, 2020). The ability to share current COVID data among other professionals in the field, where new, vital information may be released, is extremely important. Similarly, the waiver targeted towards mobile testing sites is necessary for patients to receive rapid COVID testing. Overall, these waivers help treat patients quicker during a time where every minute is crucial.

On a similar note, during the beginning of the pandemic, many patients were forced to be tested, treated, and screened at different hospitals and clinics. As a result, safe health exchange is needed, and that could be more easily attainable with increased leniency—ad hoc policies such as the HIPAA waivers would increase leniency in exchanging the health data. The HIPAA waivers would also resolve the issue of people being treated in clinics that extend across different states.

These waivers are also arguably necessary to improve quality of care. In fact, Chinmoy Bhate MD, a dermatologist at Rutgers New Jersey Medical School, recognizes that "patient care may be compromised when health care providers disproportionately fear the consequences of HIPAA violations." This concept is referred to as the "code of silence" (Bhate, 2020, p. 1). So, with less focus on HIPAA violations, physicians can direct their undivided attention to treatment and communicating with their patients. Especially during a national emergency, abiding by HIPAA's normal strict laws may be the last thing on physicians' minds. However, patient data can unintentionally be leaked since privacy takes a back seat. But the opposite also holds true. Knowing that their private health information might not be protected, patients may be less willing to share that information with their physicians in the first place, which hurts patient-physician communication and quality of care. Should the OCR and HHS have loosened HIPAA regulations to allow for immediate and simpler physician-patient interaction? Absolutely, but there should have been better planning from the government's end and should not have been so poorly executed. Consequently, HIPAA waivers have compromised patient privacy at an unacceptable level.

March 13th Waiver

In order to prove the inadequacy of HIPAA during the pandemic, the language and gaps of each waiver must be examined individually. The World Privacy Forum, a non-profit group directed towards privacy-related issues, published a journal on the specific HIPAA waivers written by Robert Gellman, a "privacy and information policy consultant in Washington DC," and Pam Dixon, the "founder and Executive Director of the World Privacy Forum" (Gellman, 2020, p. 2). On March 13, the Secretary of the HHS waived penalties with regards to noncompliance on the five sections of HIPAA that are generally flexible during national emergencies (Gellman, 2020, p. 5). These 5 sections are included in HIPAA's privacy rule and briefly are: the requirement to have permission to speak with the patient's family or friends, respect requests to opt out of the facility directory, share a notice of privacy practices, allow the patient to request privacy restrictions, allow patients to request confidential communications (Gellman, 2020, p. 9). Gellman and Dixon argue that the waiver leaves a lot of legislation up to interpretation and wrongly applies an emergency-modified version of HIPAA to COVID. When waivers were enacted in the past, they were because of natural disasters that were limited by geography (Leventhal, 2020). However, COVID is a transborder virus that doesn't know the difference between rural and urban and doesn't limit itself geographically. So then, does it make sense to apply a natural-disaster waiver to a global pandemic? A conventional HIPAA waiver is usually a consequence of a temporary natural disaster; however, COVID-19 does not fit that criteria. The question if HIPAA waivers that apply to temporary, confined natural disasters can apply to a global pandemic raises valid arguments. In fact, why does the HHS and OCR seem to have a one-size-fit-all approach to HIPAA modifications to, metaphorically, different sized disasters?

Looking at the language, the last clause states that the waiver applies "only with respect to hospitals in the designated geographic area that have hospital disaster protocols in operation during the time the waiver is in effect" (Gellman, 2020, p. 12). However, this raises new concerns. The authors note that COVID-19 is a nationwide pandemic that knows no borders, so a "designated geographic area" is difficult to maintain, since these areas are constantly changing (Gellman, 2020, p. 12). On one side, it may be inappropriate and unfair to non-COVID patients to waive privacy regulations in an area with few COVID-19 patients; however, without waiving those restrictions, tracking and recording data on the pandemic is difficult, so the case specifics in undesignated areas would be harder to report. Until the specifics of the virus itself is clear, it is difficult to differentiate when and where the waivers should apply, since HIPAA waivers currently operate at an "all or nothing" approach. Hopefully when the symptoms of COVID-19 are completely understood, the HIPAA waivers will only apply to COVID patients rather than all patients receiving treatment.

Second, Gellman and Dixon report that there is no definitive timeline on when the pandemic is over, so it is unclear how long the waiver will be "in effect" (Gellman, 2020). In this case, imposing permanent expectations for different scenarios and types of emergencies that affect healthcare administration seems to be a better solution rather than imposing vague, temporary waivers that are applied in every situation. Also, the authors note that limiting the waiver to only "hospitals" discounts other comprehensive healthcare providers for COVID patients since hospitals are not the only places where COVID patients can be treated (Gellman, 2020). By waiving some of the HIPAA requirements for all patients, it is unfair for "many patients receiving treatment [that] do not have COVID-19, and....waiving their privacy rights [may be] inappropriate" (Gellman, 2020, p. 11). All of these linguistic caveats show how difficult the waiver is to apply to the global pandemic.

In specific, this March 13th waiver, as mentioned, waived five specific HIPAA regulations that could be employed for noncompliance. The fifth penalty, "the patient's right to request confidential communications" is the most imposing on patient privacy (Gellman, 2020, p. 11). Patient requests should be taken seriously, especially with regards to their privacy. Again, it is important to remember that this provision applies to *all* patients, regardless of their COVID history. That being said, a request to keep conversations confidential in the cases of rape, domestic violence, adolescent inquiries about sexual activity, should not be waived. Although those conversations would most likely not be shared, healthcare professionals should not be given the option to be able to. Looking at this exhaustive breakdown of the March 13th waiver—the first set of regulations to be waived in any emergency—shows gaps where patient privacy can be exposed and where the legislation should be clarified.

Three Remaining HIPAA Waivers

Continuing on to the next three waivers passed, it becomes more apparent how patient privacy becomes less of a priority. The telehealth waiver, passed on March 17, waived potential penalties, regardless of its relation to COVID, on communication platforms such as Facetime and Skype made in "good faith." (Gellman, 2020). In the immediate demand for telehealth, platforms such as Skype and Facetime had to be permitted. However, ambiguity surrounding the idea of possible data breaches and the extent to which the waiver applies will require more clarity once the pandemic passes. Similarly, it is important to recognize the hesitation when using these platforms. In discussion about the three large video-conferencing companies—Cisco, Microsoft, and Webex—"all three companies can collect data while you're in a videoconference, combine it with information from data brokers and other sources to build consumer profiles, and potentially tap into the videos" (St. John, 2020). This can be devastating if they misuse patient information and create profiles of people since these technology platforms aren't held to the same HIPAA

standards. With telehealth comes a reliance on technology, and if those systems have opportunities to steal information off of video conferences and are also not subjected to HIPAA, one can imagine the possibilities of privacy breaches. Rebecca Herold, CEO at Privacy Professor and who has over 25 years of experience in privacy, argues that one "must balance security [as it relates to technology systems] with convenience," and although encryption may be "difficult and expensive to deploy...it might be a necessary evil" (Herold, 2015, pp. 338-339). With this in mind, although platforms such as Facetime, Skype, and Zoom might be significantly more convenient for patients and physicians alike, especially now, managing a HIPAA compliant technology system that prioritizes privacy is necessary.

To delve in deeper into the more ambiguous of the three waivers, the Business Associate waiver of April 2 states that it will not penalize business entities for "good faith uses and disclosures" of Protected Health Information (PHI) (U.S. Department of Health & Human Services, 2020). One phrase is used in all three of these waivers: "good faith." But good faith is largely subjective, and the lack of a clear definition can create gaps in compliance because of differences in understanding. This "up-for-interpretation" approach is problematic for business associates because they are not as familiar with patient privacy regulations as healthcare providers, they are not held to the same ethical standards, and lack detailed knowledge about the current pandemic. In the name of providing quicker access, the HHS "now permits business associates to also share [COVID-related] data without risk of a HIPAA penalty" (U.S. Department of Health & Human Services, 2020). But this extension of the waiver now allows far-removed business associates such as, "paper shredding services; website hosting and management services; mobile app providers" to have access to the same information as companies that manage a hospital's electronic health record (Gellman, 2020, p. 16). Moreover, if the PHI is shared with entities that are not covered by HIPAA, the privacy rule no longer applies; this greatly exposes patient privacy if PHI is put into untrusted hands justified by flexible "public health purposes." But health information is bound to be shared. For example, COVID "patients may first be screened by one organization utilizing telehealth, obtain testing at a 'drivethrough' collection site run by a second institution, have tests performed by one of multiple clinical laboratories with novel testing capacity, [etc.] not necessarily related to any prior providers in the information chain" (Lenert, 2020, p. 1). Now more than ever, safe health information exchange is needed.

One of the largest problems with the Business Associate waiver is that "there is no requirement that a business associate either have or rely upon professional expertise in making decisions about data use and disclosure for public health or health oversight purposes" (Gellman, 2020, p. 16). This means that business associates, who have no expertise in public health, are given the authority to judge "good faith" and disclose patient

information to entities that don't necessarily need that information (Gellman, 2020). A more concise tracking system, where no matter who owns PHI, HIPAA applies should be implemented; if PHI is shared with non-HIPAA covered entities, HIPAA should continue to impose regulations on how that patient data is distributed. In addition, "public health or health oversight purposes" needs to be further clarified. With vague language, it is easy to find loopholes and manipulate the legalese into one's favor, not always in agreement with what the patient wants. In Gellman and Dixon's final remarks about the Business Associate waiver, they assert that, "if grades were awarded for the quality, necessity, and responsibility of waivers, the Business Associate waiver would receive a failing grade" (Gellman, 2020, p. 19). The lack of thorough legislation within the waiver, coupled with the vague and unclear language used, creates opportunities for privacy violations and legislation manipulation.

And lastly, on April 9, the Community Based Testing Sites (CBTS) Waiver was passed; this waiver pertained to mobile COVID-19 testing sites and similarly stated that the OCR will not penalize testing sites with noncompliance made in "good faith" (Gellman, 2020). This waiver was crucial for fast mobile testing and helped meet the demand for testing sites. Fortunately, the OCR put in place specific guidelines for CBTS such as, sharing the minimum amount of PHI, imposing social distancing policies at the sites to help limit contact and eavesdropping, and securing technology systems (Gellman, 2020). Leslie Lenert, a professor at Medical University of South Carolina who has dedicated his studies towards medical bioinformatics, provides a counterargument to the idea of "minimum" during COVID. He believes that "transmission of minimal information [should] not apply to public health entities during this crisis. [In fact,] public health officials should have unfettered access...for case investigation and patient care" (Lenert, 2020, p. 3). However, currently when "minimal" is not defined or restricted, "unfettered" access would pose even more risks to patients. Like with the other waivers, "good faith" and "encouraged" provisions do not seem mandatory or restricting. It's easy to argue "good faith" purposes and, at the local level, it can be easy to not follow "encouraged" measures to prioritize patient privacy.

Other Models and Examples

Considering the COVID-19 pandemic is recent, not a lot of scholarship has been published on the niche topic of HIPAA during COVID. In order to compare the balance between public interest and individual privacy, I analyze Taiwan, a successful country in handling the virus and cases. It is important to note the cultural differences in how privacy is handled internationally; although many Asian countries have similar laws regarding privacy, in a cultural sense, personal privacy and strict limitations are not as prioritized like they are in the United States. Wei-Ting Yen PhD, an assistant professor of government at Franklin and Marshall College, who studies political economy issues in the developing

world, especially across Asian countries, has conducted research in this area. One driving force of loosening HIPAA's regulations is the need for researchers to analyze the effectiveness of contact tracing, social distancing, quarantining, etc; however, a lot of this research is restricted by HIPAA's requirement on anonymity of clinical data (Lenert, 2020). From this, it is clear that HIPAA or the HHS and OCR need to redefine what protected health information is in the context of a pandemic. Coined as the "big data" approach, there has been controversy on what the government's role should be in drawing the line between supporting public interest during a pandemic and individual privacy.

Originally, because of its proximity to China, many people believed Taiwan would be hit hard by the virus. But one factor that has resulted in Taiwan's surprisingly low case amount is how the government regulated big data and its transparency between citizens and authorities, otherwise known as an "effective digital governance regime" (Yen, 2020, p. 8). Taiwan, unlike the United States, didn't have the barrier of "anonymity of clinical data." They relied on "digital governance [to help] improve disease detection through integrated databases of people's health records and travel history, through more accurate contact tracing, and through active surveillance tracking for people under quarantine" (Yen, 2020, p. 80). This is a stark contrast from how the United States handled the publishing of patient data, or the lack thereof.

In Taiwan, there is a strong relationship between the National Health Administration and Customs; they have connected "individual international travel history to the national health insurance system" (Yen, 2020, p. 8). Authorities track quarantined people's locations through GPS systems based on a list generated by the CDC; if the person couldn't be reached, alarms would be triggered, and they would receive an in-person visit by the local authorities (Yen, 2020). This model may not be well-received in America, where this would be perceived as abridging individuals' freedoms, and this would be a far-reaching change to HIPAA. Americans demand and expect privacy; the average American doesn't know the details of what is protected and not under HIPAA because they trust the government. In Taiwan, although this approach was successful, "active digital surveillance tools raised substantial concerns about individual privacy" (Yen, 2020, p. 9). Part of Taiwan's success in combating COVID-19 was the government's direct involvement with patient data, publicizing that data for local authorities, and Taiwan citizens contributing to their own surveillance by following the imposed tracking methods—a different type of trust in the government. This shows an extreme possibility, where patient privacy is not the priority, and HIPAA is an after-thought. In Taiwan, tracking individuals certainly crosses privacy lines, and they justify that by the much smaller number of cases (Several sources confirm that as of November 4, Taiwan has had a total of 568 cases).

Another country the United States could get inspiration from is Singapore, a country with government intervention but not as much as Taiwan. Hyunghoon Cho, a Schmidt Fellow at the Broad Institute of MIT and Harvard, studies computation in the context of biomedical data. On March 20, 2020, Singapore launched a contact tracing app called TraceTogether. This app tracks users, allows individuals to report if they have been tested positive with COVID, and notifies users when they have come in contact with COVID patients (Cho, 2020). This app has shown great levels of success. However, its potential success in America is debatable. Although "a public health emergency could well be argued to be a valid cause...many Americans are wary of sharing location and/or contact data with tech companies or the government" (Cho, 2020, p. 1). On a similar note, these tracing apps may be difficult to implement in the United States because it would require a mandate of some sort. The installation of the app could be employed as an implied consent law for public places (Cho, 2020). Requiring the installation of an app in certain places would help public interest, but not so many scientists and researchers since people would only have this app "on" in certain areas. The anonymity of the app protects individuals, but does not advance the goal of a better understanding of COVID from a science perspective. In the United States, if an app for contact tracing is mandated, anonymity is key to protect peoples' freedoms and privacy.

Lenert provides a similar perspective on contact tracing and HIPAA. He comments that cellular applications and research to examine home quarantines, social distancing strategies, and avoidance of large gatherings are "urgently needed in order to direct policy—but much of this work is limited by current federal requirements" (Lenert, 2020, p. 1). In order to follow the model of other successful countries, the United States would have to "[loosen] the borders of anonymization [to allow] data scientists [to have] access to the information without administrative barriers." This will require "changes to the definition of what protected health information (PHI) is, in the context of this epidemic" (Lenert, 2020, pp. 1-2). I think Lenert makes a valid argument in that PHI needs to be redefined. Rather than blanketly waiving HIPAA violations, the government should clearly state what health information is protected and not, so it is not up for interpretation among businesses and healthcare providers, nor is there a need to rely on "good faith." However, it can be argued that there are not many "administrative barriers." In fact, as discussed, the waivers make HIPAA lenient and harmful to patient privacy. Broadening anonymization to more than "good faith" and dismantling HIPAA regulations will further compromise patient privacy. In this situation, it is important to find the right balance between health information exchange and research. Specific guidelines should be written rather than more vagueness. It is important to note that I do not argue that the United States should follow Taiwan and Singapore's models regarding heavy government involvement. I think the balance between public

interest and individual privacy lies in defining terms and closing gaps in legislation, not making privacy a secondary concern and disrupting confidentiality inefficiently like in Taiwan, Singapore, and in the situation Lenert proposed.

Recommendations

This next section of the paper will outline several different recommendations taken from authors involved in the field. Eric Thompson, author of the book *Building a HIPAA-Compliant Cybersecurity System* and many other publications about the intersection of cybersecurity and health privacy, Thompson is a qualified expert on security systems and HIPAA. In his publication, Thompson introduces the importance of conducting a risk analysis, which lists potential vulnerabilities in the cybersecurity system, the probability of them being exposed, and its consequential impact (Thompson, 2017). Thompson argues that not conducting a risk analysis is a waste or underutilization of cybersecurity and advanced technology in healthcare (Thompson, 2017). Secondly, he argues for a switch in mentality in approaching HIPAA as a comprehensive method to protect patient privacy—he does so with the claim of improving cybersecurity systems—rather than boxes needed to be checked off. He coins this as an "offensive approach" to patient privacy rather than a "defensive" one. Knowing that HIPAA was written when patient data was recorded on paper, the OCR and HHS should work hand-in-hand with cybersecurity teams, computer scientists, and engineers to help design and implement strong programs to ensure privacy. Using technology to their advantage, it will be even more important for hospitals to manage their patient records during the pandemic era. Similarly, according to Nicole Martinez-Martin—a psychological anthropologist and bioethicist—privacy regulations should have four key focuses: transparency, informed consent, privacy, and accountability (Martinez-Martin, 2018).

Another recommendation that should be considered, even for post-COVID, is training. With the complex legalese of HIPAA, it is often difficult for healthcare professionals to decipher where lines should be drawn with regards to patient privacy and security. Most privacy breaches begin with phishing emails, and with the rise of social media, it has become easier for attackers to create individualized emails that seem more legitimate. Thompson urges medical professionals to undergo training on HIPAA and how to recognize these emails and messages (Thompson, 2017). This will strengthen the relationship between medical personel and the legislation itself. For COVID-19, it will be beneficial for healthcare workers to understand how HIPAA was modified and what the consequences are of those changes; similarly, a better understanding of the HIPAA waivers will help healthcare providers recognize privacy breaches ahead of time and gaps where patient privacy may be compromised.

Looking back to the March 13th waiver, one recommendation to reduce the vagueness is to define what constitutes a "designated geographic area." A baseline number considering the amount of positive cases to identify high risk areas, rather than "designated" areas may prove beneficial since there is a give and take with labeling an area as "high risk" or "designated." This would help recognize where HIPAA waivers should be more emphasized and where HIPAA waivers may not be as necessary. In regard to the same waiver, as mentioned earlier, the HHS waived the fifth penalty that is the requirement to allow patients to request confidential communications. The HHS should rewrite the provision to include exceptions or specifically mention that these provisions will only be waived with COVID cases, rather than compromising non-COVID patients' privacy.

An underlying theme of all waivers is: good faith. In order to decrease potential breaches, the OCR and HHS should institute a way to measure and recognize good faith. Especially with the current vaccination rollout, healthcare providers should be comfortable enough with the waivers to not need good faith measurements. Legislation should be implemented to better define consequences and the waivers themselves to ensure privacy is prioritized.

Looking Forward

These temporary changes prompt the question about what patient privacy will look like after the pandemic is over. "Matt Fisher, the chair of law firm Mirick O'Connell's health law group and a partner in the firm's business group, believes, 'Once the privacy cat is let out of the bag, it cannot be put back in.'" In other words, in the context of cybersecurity, Fisher believes that "'patient data hosted or stored in a non-HIPAA compliant platform could end up being used for a number of unexpected or non-desirable purposes'" (Levanthal, 2020). The leniency of HIPAA must be compensated in the technology platforms used, whether it be tightening up loose ends in cybersecurity systems, or just ensuring that telehealth platforms are HIPAA-regulated. As discussed earlier, these major video-conferencing platforms can steal patient information, and with these new waivers, not much can be done to guarantee that information will stay confidential. When designing cybersecurity systems in the future, it will be important to plan for and consider the transition from pandemic-telehealth to post-pandemic health institutions.

There seems to be a consensus among scholars that telemedicine is here to stay even after the pandemic passes. David Klonoff, a practicing endocrinologist specializing in diabetes technology, wrote an academic journal concentrated on telemedicine. He argues that telemedicine will become more integrated in healthcare and "although there will always be a tension between access and privacy...HIPAA will be rewritten or reinterpreted to better promote telemedicine care." And despite telemedicine's benefits, a "data tsunami [of patient records] will increase

the risks of data breaches and require sound cybersecurity protection" (Klonoff, 2020, p. 2). This brings the conversation of how HIPAA should move forward to how technology systems can protect privacy. Cho explains if the government is "willing to invest in additional computational resources, it is possible to achieve increased privacy from snoopers, contacts, and the authorities." Although more "expensive, [it] would assure users that they do not have to give up their privacy in order to take part in public contact tracing efforts…[perhaps this] guarantee would go a long way towards mass adoption of a contact tracing app in the United States," following countries such as Taiwan and Singapore (Cho, 2020, p. 9).

Additionally, a newly implemented strategy is contact tracing apps, which were heavily used worldwide to combat the virus and community transmission. With the same goal of efficiently using patient data without as many restrictions, contact tracing apps were implemented to help with case identification and data collection and comparison. In May 2020, Apple and Google jointly launched Exposure Notifications, which relied on Bluetooth signals. The program has a questionnaire that assesses a person's need to be COVID-tested. However, in order to take the questionnaire, the person must provide their Google account information, which can be shared with third parties. But the largest issue with this tool is the Google and Apple are not held to HIPAA standards because they do not offer medical devices and are not medical companies; in fact, this applies to most Big Tech companies, who also are not regulated by federal privacy regulations but have accumulated large amounts of health data from users. Contact tracing apps provide another perspective of where gaps in HIPAA lie and the need for this legislation to adapt to the digital era.

In order to recognize the inadequacy of HIPAA during COVID-19, it is important to identify what has already been done and what its consequences are. As a relatively new field to explore, there haven't been many studies on the consequences of lenient laws during COVID-19. However, analyzing the legislation itself provides a look into speculations and where patient privacy is exposed. After reading the waivers, it becomes clear that both the lack of adequate legislation and vague language used has compromised patient privacy to a point where it no longer justifies public interest. I have pointed out areas for clarification and improvement in the legislation and hope these concerns are taken seriously. Patient privacy is important to every person receiving treatment. The promise to keep health data confidential, is also a promise of protecting the person's autonomy and dignity, and guarantees mutual respect and avoids discrimination; a forgotten promise during the current COVID-19 pandemic.

References

Bhate, C., Ho, C. H., & Brodell, R. T. (2020). Time to revisit the Health Insurance Portability and Accountability Act (HIPAA)? Accelerated telehealth adoption during the COVID-19 pandemic. *Journal of the American Academy of Dermatology*, *83*(4), e313–e314. https://doi.org/10.1016/j.jaad.2020.06.989

Cho, H. Ippolito, D., & Yu, Y. W. (2020). Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs. *ArXiv,* 1-12. https://arxiv.org/pdf/2003.11511.pdf

Gellman, R., & Dixon, P. (2020). COVID-19 and HIPAA: HHS's Troubled Approach to Waiving Privacy and Security Rules for the Pandemic. *World Privacy Forum.* www.worldprivacyforum.org/2020/09/covid-19-and-hipaa.

Herold, R., & Beaver, K. (2015). The practical guide to HIPAA privacy and security compliance. *Auerbach Publications.* https://learning.oreilly.com/library/view/the-practical-guide/9781439855584/

Health insurance portability and Accountability act of 1996 (HIPAA). (2018, September 14). Retrieved March 29, 2021, from https://www.cdc.gov/phlp/publications/topic/hipaa.html

Klonoff, D. C. (2020). Telemedicine for Diabetes After the COVID-19 Pandemic: We Can't Put the Toothpaste Back in the Tube or Turn Back the Clock. *Journal of Diabetes Science and Technology*, *14*(4), 741–742. https://doi.org/10.1177/1932296820932958.

Lenert, L., & McSwain, B. Y. (2020). Balancing Health Privacy, Health Information Exchange, and Research in the Context of the COVID-19 Pandemic. *Journal of the American Medical Informatics Association*, *27*(6), 963–966. https://doi.org/10.1093/jamia/ocaa039.

Leventhal, R. (2020, March 19). *HIPAA and COVID-19: Restrictions Loosened, But Experts Preach Caution.* Healthcare Innovation. https://www.hcinnovationgroup.com/covid-19/article/21130404/hipaa-and-covid19-restrictions-loosened-but-experts-preach-caution.

Nicole Martinez-Martin, Thomas R. Insel, Paul Dagum, Henry T. Greely, & Mildred K. Cho. (2018). Data mining for health: staking out the ethical territory of digital phenotyping. *Npj Digital Medicine*, *1*(1), 1–5. https://doi.org/10.1038/s41746-018-0075-8

St. John, A. (2020, April 30). *It's Not Just Zoom. Google Meet, Microsoft Teams, and Webex Have Privacy Issues, Too.* Consumer Reports. https://www.consumerreports.org/video-conferencing-services/videoconferencing-privacy-issues-google-microsoft-webex/.

The New York Times. (2021, March 28). Coronavirus in the U.s.: Latest map and case count. Retrieved March 29, 2021, from https://www.nytimes.com/interactive/2020/us/coronavirus-us-cases.html

Thompson, E. C. (2017). *Building a HIPAA-compliant cybersecurity program: Using NIST 800-30 and CSF to secure protected health*

information. U.S. Department of Health and Human Services. (2020, April 2). *OCR Announces Notification of Enforcement Discretion to Allow Uses and Disclosures of Protected Health Information by Business Associates for Public Health and Health Oversight Activities During The COVID-19 Nationwide Public Health Emergency.* HHS. https://www.hhs.gov/about/news/2020/04/02/ocr-announces-notification-of-enforcement-discretion.html

Yen, Wei-Ting. (2020). *Taiwan's COVID-19 Management: Developmental State, Digital Governance, and State-Society Synergy. Asian Politics & Policy.* ResearchGate. 12. 455-468. https://doi.org/10.1111/aspp.12541.