The Health Insurance Portability and Accountability Act and its Impact on Privacy and Confidentiality in Healthcare

Allyssa Stadler

A Senior Thesis submitted in partial fulfillment
of the requirements for graduation
in the Honors Program
Liberty University
Spring 2021

Acceptance of Senior Honors Thesis

This Senior Honors Thesis is accepted in partial
fulfillment of the requirements for graduation from the
Honors Program of Liberty University

_____

Jeong-Ho Kim, PhD
Thesis Chair

_____

Gary Isaacs, PhD
Committee Member

_____

Cynthia Goodrich, EdD
Assistant Honors Director

_____

Date

Abstract

The world of healthcare and technology has continued to grow and expand into the future while HIPAA (the Health Insurance Portability and Accountability Act), the foundational patient privacy law in the United States of America, is attempting to keep up with this new world. This thesis reviews HIPAA and other health-related laws necessary to understanding patient privacy. It analyzes peer-reviewed studies on patient confidentiality and HIPAA to elicit the patient's and provider's opinion on HIPAA and patient confidentiality. Lastly, the current challenges of patient confidentiality and HIPAA are discussed, and potential solutions are suggested to improve these issues.

HIPAA (which stands for the Health Insurance Portability and Accountability Act of 1996) can feel complicated and unclear to some. Understanding HIPAA first is crucial in having a discussion on patient confidentiality in the United States. It is a Public Law that contains requirements for combating fraud in health insurance and health care, simplifying health insurance administration, and developing guidelines for patient privacy, security, health information systems and how they will be electronically transferred (Health Insurance Portability and Accountability Act, 1996). More than 20 years after HIPAA became a law, it continues to be updated and modified with respect to its application. Because of these changes and the complicated nature surrounding HIPAA laws and rules, healthcare professionals, patients, administrators, and others in the general public would benefit greatly from a review of HIPAA's rules, opinions from providers and patients, and the issues that have arisen when implementing HIPAA in hospital/clinic policies. The goal of this review is to help the public become more educated on the requirements and rules under HIPAA, patient rights, and the use of patient health information.

Methods

Peer-reviewed studies, case-studies and reviews were chosen in the following databases: the Liberty University library journal article database (an academic division of ProQuest) under the peer-reviewed category, scholar.google.com, and the PubMed databases. All literature concerning the laws spoken of in this thesis were found on the Department of Human Health and Services website, other official resources, or resources to access the full text of the laws and regulations. Lastly, some opinion papers were used in order to elucidate opinions of providers and experts as supplement to the peer-reviewed studies. Example searches done included

"patient opinion of confidentiality," "opinions on patient confidentiality," "HIPAA and patient opinions," and "patient opinion on HIPAA."

Literature Background

HIPAA and Healthcare Law Background

HIPAA (original law)

There are five titles (sections) within the original HIPAA law (see Table 1). The first title is "Health Care Access, Portability, and Renewability" (HIPAA, 1996). This title consists of guidelines for health insurance companies and employee health insurance. The second title is "Preventing Health Care Fraud and Abuse; Administrative Simplification; Medical Liability Reform." The section on preventing fraud and abuse is focused on requiring more investigations, increasing documentation, and increasing refunds within healthcare. The administrative simplification part of this title refers to the requirements put in place for the Department of Health and Human Services (HHS) to create future rules and standards for privacy, transactions and code sets, security, unique identifiers, and enforcement (such as the Privacy Rule, Security Rule, and Enforcement Rule). The third part of the second title is medical liability reform. This is related to the fraud and abuse prevention because decisions on liability and the introduction of liability insurances are now needed due to new penalties when fraud, abuse, or inappropriate disclosure occurs. The third title is "Tax-Related Health Provisions Governing Medical Savings Accounts [MSA's]." This reference to savings accounts is a special account available to employees under their employer or self-employers that has money automatically deposited in for various medical expenses. This title standardizes the amount allowed to be saved in these

"MSA's." Title four is "Application and Enforcement of Group Health Insurance Requirements." This is specific to health plans for those with pre-existing health conditions and clarifies the requirements. Title five is "Revenue Offset Governing Tax Deductions for Employers." This is centered around life insurance that is company owned and prohibiting tax-deductions of these life insurance payments. These five titles make up the original HIPAA law of 1996 and would soon lead to new Rules put in place by the HHS.

Table 1

The Five Titles in the Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Title I	Health Care Access, Portability, and Renewability	Insurance company guidelines
Title II	Preventing Health Care Fraud and Abuse; Administrative Simplification; Medical Liability Reform	Future rules regarding privacy and fraud are to be put together by the HHS and are to be adopted and followed by all in the U.S.
Title III	Tax-Related Health Provisions Governing Medical Savings Accounts	Rules and guidelines surrounding MSA's
Title IV	Application and Enforcement of Group Health Insurance Requirements	Specific insurance company group guidelines for those with preexisting conditions
Title V	Revenue Offset Governing Tax Deductions for Employers	Life insurance guidelines

The Privacy Rule

When many people think of HIPAA, especially when it is related to patient confidentiality, they usually are thinking of the guidelines in the Privacy Rule. This rule was created by the HHS based on the requirements set forth in Title II of the HIPAA law. It is the national standard for protection of health information. This is called "protective health information" or PHI and is all identifiable information. A balance is made of protecting the privacy of people and still disclosing when it is important. An important part of the Privacy Rule

includes the right for patients to access their healthcare information such as charts, images, and diagnoses. The Privacy Rule introduces many terms and ideas that need to be defined. First, there are three different entities discussed, the patient, covered entities, and business associates. A covered entity is described as a health care provider, health plan (i.e. insurance companies), or a healthcare clearinghouse. All of these companies and providers are required to follow HIPAA guidelines. In comparison, business associates are persons or entities that provides services for covered entities and/or are handling protected health information on a covered entity's behalf. (Summary of the HIPAA Privacy Rule, 2008; Business Associates, 2009a). Healthcare professionals and other "covered entities" and "business associates" are able to use and share a patient's PHI without consent when it is being used for "treatment, payment and operations of health-care related activities" (Security and Privacy, 2002).

Security Rule

The Security Rule is another aspect of the HIPAA regulations put in place. This accounts for protected information now being stored on computers in an electronic health record form. The Security Rule puts guidelines in place for keeping this information safe from breaches, hacking, and other things that could cause confidentiality to be breached. These guidelines include requiring certain technological, physical, and administrative safeguards. This rule is meant to protect electronic personal health information from those who should not see it while the Privacy Rule is meant to regulate who can view personal health information. Some examples of guidelines expected from this rule include authentication software, encrypted data, off-site backup computers, and new security workforce roles (Security Rule Guidance Material, 2009b).

HITECH/Breach Notification Rule

HITECH (Health Information Technology for Economic and Clinical Health) was a recent (2009) modification done to HIPAA that strengthened the previously nonthreatening regulation. After years of the HHS not enforcing HIPAA, many covered entities and business associates were no longer concerned with compliancy. This modification quickly changed that mindset. The monetary amount that the HHS could now require for violations of HIPAA regulations dramatically increased up to a million dollars in some circumstances (Solove, 2013). As well, HITECH added the requirement for entities and associates to send notifications to affected parties when breaches in PHI were detected. This is now usually known as the Breach Notification Rule. This rule came at a time when more and more technology breaches of personal information were happening. This rule hoped to create transparency and serve as a way to alert patients of possible medical identity theft. These notifications must happen individually through email, or physical signed notice and also may be required to go to the media in the case that a large number of persons are affected by the breach (>500) (Breach Notification Rule, 2009).

Enforcement Rule

In 2006, the Enforcement Rule was passed, and organizations were given two to three years to comply with these new guidelines on fees and penalizations. However, only one year later, the HITECH rule was passed which immediately overhauled the Enforcement Rule and thus, the Enforcement Rule is not as well known due to it being overshadowed by the HITECH rule. All of the new regulations regarding penalties and fees within the HITECH rule are modifications to the Enforcement Rule (Enforcement Rule, 2008).

Final Omnibus Rule

The Final Omnibus Rule in 2013 consisted of changes to the HITECH rule that strengthened privacy and security protections (Omnibus HIPAA Final Rule, 2013). It increased some of the monetary penalties under the HITECH rule. As well, it changed rules under Breach Notification to instead presume a breach unless proof was shown that there was not a compromise compared to the original which was providing evidence to prove a breach. Next, changes were made to coincide with GINA (see Figure 1, page 11) in order to prohibit health plans from using genetic information wrongly. Next, HITECH was modified to allow patients to pay fully out of pocket and instruct the provider to not share information with their health plan. Next, the law was changed so that business associates would receive the same fines and penalties that covered entities do. Finally, the Omnibus Rule allowed for providers to directly share patients' vaccination records with schools once they receive release from a guardian or parent and prohibited any marketing, fundraising, or sale of PHI without authorization.

Proposed Modifications to the Privacy Rule

From 2019 up to the present, there have been more modifications to the privacy rule being proposed. These modifications will help create better interaction with patients, remove any regulatory obstacles to providing coordinated care (which means what one would think, coordinating care amongst providers of a patient to give the safest and most quality care for their patient), and update HIPAA and the Privacy Rule to account for more recent problems that need to be solved. The Privacy Rule would be updated with the definition of electronic health record (EHR) which is currently not in the Privacy Rule or HIPAA. The proposed definition would specify that an EHR in the case of HIPAA and privacy only refers to the part of the EHR software that contains health-related patient information (because EHR software often also

contains appointment, billing, and other business-related management). It would also change the requirements of obtaining a written acknowledgement from a patient that they received their Notice of Privacy Practices. Instead, the patient would be given the right to discuss the NPP with a designated person, and the actual NPP would be reworked to help educate patients better on their rights and the entity's privacy practices. The possible Privacy Rule modifications would also help remove obstacles when coordinating care by changing the role of Telecommunications Relay Services communications assistants from business associates to expressly being permitted to have information disclosed to them without a business associate agreement. As well, a large part of these modifications are helping patients to access their PHI more easily by strengthening their rights. This includes being allowed to take notes or photograph their PHI, shortening the response time of PHI access requests for covered entities, better clarifying the expectations for requesting PHI, reducing identity verification burden, and officially requiring providers and health plans to respond to record requests from other covered entity providers and health plans. As well, health care operations would be clarified in order to include care coordination which is further clarified to consist of things like social services, or home and community-based service providers. Therefore, disclosing this information does not (and is clarified that it would not) require patient consent. Another aspect of these modifications is changing the wording of when a covered entity can disclose PHI to avert a threat from "serious and imminent threat" to the new wording, "serious and reasonably foreseeable" (Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement, 2021). This would better allow providers to release patient information in good faith to authorities or other appropriate persons when they believe their patient is a danger to themselves or others.

This could be very good for the public so that covered entities feel freer to notify authorities before things escalate or someone gets hurt. On the other hand however, some patients could see this change and not feel safe to share all of their health information, especially if it is mental health or substance related. Lastly, it is also proposed that more clarifications be done to encourage covered entities to disclose information to family and caregivers when they are attempting to assist the individual in an emergency, a SUD or SMI. This disclosure would also be in good faith belief instead of an exercise of professional judgement (Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement, 2021). These modifications are currently under review and taking comments from the general public (ends May 6, 2021). After this stage, the proposed modifications will be considered, and more changes will be done to the proposal before becoming a final rule (News Division of HHS, 2021).

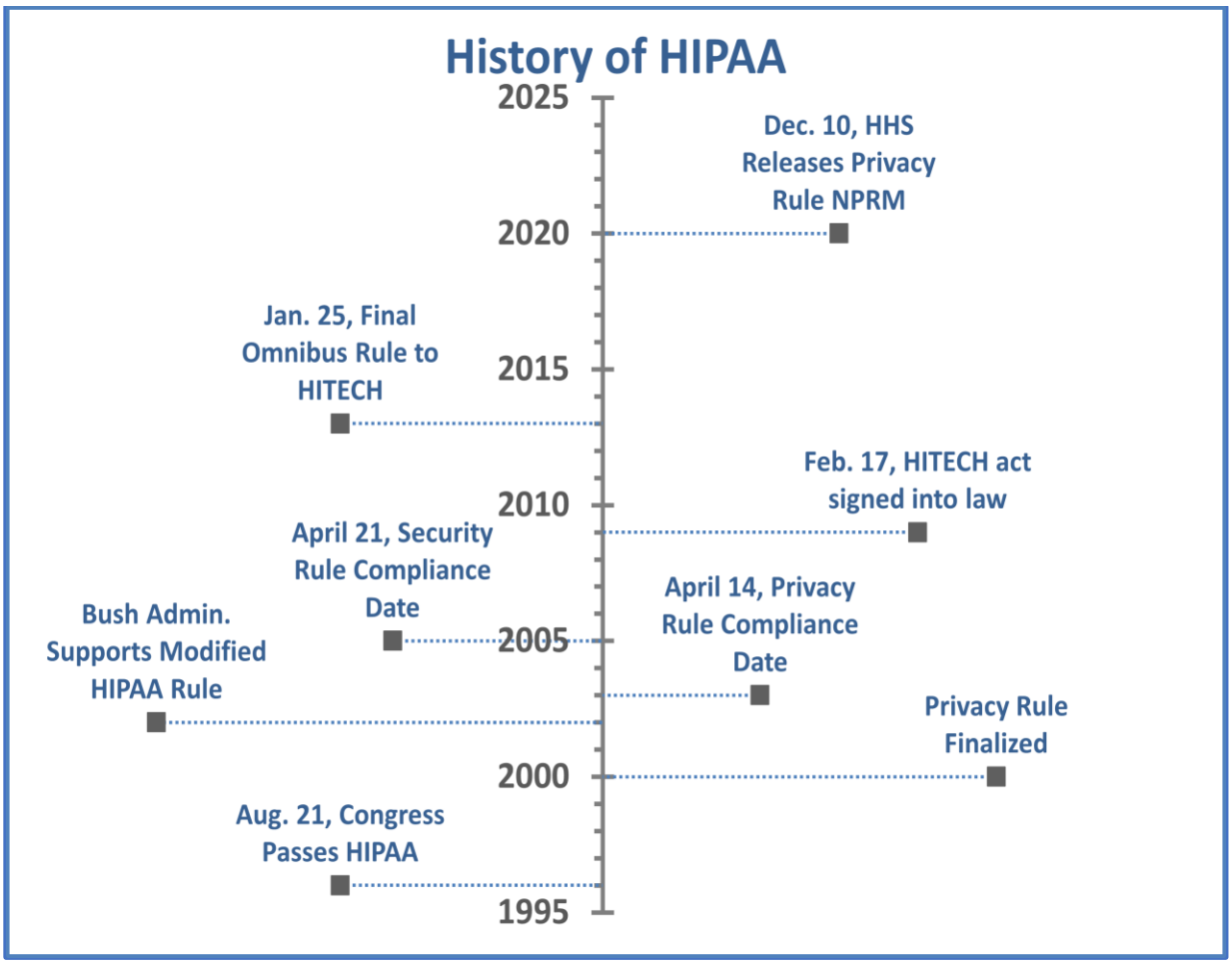

Figure 1. The history of HIPAA and all the subsequent rules following up to the present day are presented (Summary of the HIPAA Privacy Rule, 2008; Security Rule Guidance Material, 2009b). Keeping track of the dates and order of these important events helps to better understand the current HIPAA guidelines in place. Not included in this timeline is the Enforcement Rule compliance date due to the almost immediate modifications of it put in place by the HITECH act (Enforcement Rule, 2008). Based on previous information, it can be expected for the current Notice of Proposed Rulemaking to become a law in the next two to three years (U.S. Department of Health and Human Services, 2021). The template for this figure was accessed using Microsoft Office (*Vertical timeline,* 2020).

COVID-19 and HIPAA

HIPAA and patient privacy cannot be seriously discussed without addressing how the COVID-19 pandemic has been affecting them. COVID-19 has introduced a myriad of new situations that have caused the HHS to issue new guidelines. These guidelines prioritize the needs of patients and providers during the pandemic over certain rules and guidelines within HIPAA. For instance, currently there is a lot of enforcement discretion occurring in relation to temporary testing or vaccination sites, new telehealth communication options, public health activities, contacting previous COVID-19 patients to inquire about convalescent plasma donation, and others (HIPAA and COVID-19, 2020). These new situations have warranted this enforcement discretion in order to stop more confusion and uncertainty as covered entities are stepping into unknown territory that may not fit the guidelines or rules currently set up in HIPAA.

Guidelines of following the Privacy Rule

There are many guidelines to patient confidentiality within the Privacy Rule, Security Rule, and Breach Notification Rule and these guidelines are further explained in other sources meant to guide healthcare professionals (AMA Council, 2012; Summary of the Privacy Rule, 2008; Sabatino, 2018). These guidelines explain how there are instances where covered entities can disclose PHI to others that are not covered entities or business associates. For instance, a healthcare professional is allowed to disclose PHI when they are given consent by the patient, required by law or in the public interest. Different disclosures required by law include when ordered by a judge or court, or by a statute (i.e. child abuse). Disclosures in the public interest may include to family about communicable or genetic diseases as well as serious crimes. Other

important guidelines on patient confidentiality include those regarding minors. Parents and guardians have varying availability of the minor's health record. This availability is different dependent on if the minor is emancipated and which state the family lives in. Within reproductive and mental health, there are extra considerations that health professionals should keep in mind when attempting to give the best care. Most states have laws that allow minors to speak and make decisions with health care providers about reproductive and mental health like contraception, substance abuse, and therapy without the consent of the guardians. There are some other areas where patient confidentiality is a concern and consent is needed like in marketing or research.

Overview of Other Healthcare-Related Laws

Americans with Disabilities Act (ADA). Besides HIPAA, there are other laws in the United States regarding health care and need to be addressed when discussing patient confidentiality. The Americans with Disabilities Act speaks to accommodations required by clinics, and hospitals (ADA, 1990). These providers are required to take steps so they can effectively communicate with patients. This may include changing one's language in order to help a blind patient understand directions. Additionally, some patients with hearing disabilities may require a translator in order to effectively communicate. A translator (sign language or other language) is essential to a healthcare team and is considered a covered entity in most cases. Also, the ADA considers that insurance providers, and medical service companies are allowed under their state laws to underwrite a policy or health plan for a person who has a disability.

Genetic Information Nondiscrimination Act of 2008 (GINA). Another law related to healthcare includes GINA. This law revises HIPAA policy so that all genetic information is

considered personal health information and should not be used by a covered entity to underwrite (rule eligibility, apply an exclusion, or relating to creating, renewing, or replacing) a health plan, coverage, or policy. This is different from the ADA due to the fact that genetic predisposition is not seen as a disability or illness until a long-term illness officially arises (The Genetic Information Nondiscrimination Act, 2008). The creation of this law shows that genetic medicine patients may have specific concerns about protected patient health information which will be taken into account later (Dheensa et al., 2016). Violating this regulation would be considered violating HIPAA and could cause penalties similar to other HIPAA regulation violations (The Genetic Information Nondiscrimination Act, 2008).

Case Studies and Opinion Papers

Early Opinions of Patients and Providers on HIPAA and Patient Privacy

When HIPAA's Privacy and Security Rule went into effect in 2003 amongst the public, there were many opinions from providers, and patients on how it was going to affect the healthcare industry. Some thought it would completely halt all research, destroy the healthcare industry, and create other unsavory effects. Other privacy advocates severely critiqued the original Privacy and Security Rules expressing disappointment that HIPAA would allow business associates and covered entities to access protected health information without any knowledge or consent from the patient as long as it was for "treatment, payment and operations of health-care related activities" (Security and Privacy, 2002). They felt this was an enormous loophole that would not provide the privacy and confidentiality that was being anticipated. This change was done following the Bush administration expressing concern about the difficulty it could bring to require consent for all healthcare related activities, and the Privacy Rule was

changed based on those concerns. On the other end of the spectrum, many doctors expressed outcry at making appointment notes available to patients; they felt an ownership over their doctor's notes and perhaps that their own privacy was being invaded. Doctors and healthcare businesses were concerned they would not be able to do everyday activities in the clinic such as provide a sign-in sheet for patients or speak with families about each of their health (Solove, 2013).

An important literature review article was done in 2003 to find what the average patient thinks about health confidentiality. Not many studies had been done at that time that specifically included patients' opinions on confidentiality in relative comparison to studies about providers' opinions. Nevertheless, the available studies were analyzed to find common themes. The common themes found were that patients did not seem to understand the definition of confidentiality and what it all included, patients had more local concerns in mind like their PHI being found out by the community, patients understand they want their PHI only used during treatment and no where else, and when patients deem it necessary, they will forego important medical care, withhold information, alter their stories, or lie in order to protect their confidentiality if they believe it is at risk (Sankar et al., 2003).

There were many studies done of providers' opinions of HIPAA during this period of change in healthcare. In one, providers were surveyed in 2003 just before the compliance date in a study published in 2005. A large majority of them expressed the opinion that HIPAA was not going to improve confidentiality or the protection of confidential information. And around a third of those surveyed worried the Privacy Rule would hinder research. Interestingly, they rated organizations that are meeting the Privacy Rule standards higher than others even though they

did not believe HIPAA would improve confidentiality protection. It was suggested that this duality in their results were due to providers viewing the Privacy Rule standards as already in place before the Rule started to be implemented. This points to providers viewing the standards as good and important but already similar to what they were doing ethically and professionally but perhaps not in a regulatory manner. However, the purpose of HIPAA was due to the influx in technology and only one third of the providers in the study used an electronic medical record (EMR). Therefore, that is a factor to look at when analyzing these results. The results were concerning because the overall negative view of HIPAA that the providers had could have caused issues with implementation and that some providers would feel reluctant to share their patients' health information if they felt the regulations were ineffective (Slutsman et al., 2005). Some of the concerns providers had were (and still are) very rational and hopefully are now considered solved because of the Security, HITECH, and future Modifications to the Privacy Rule.

A study about HIPAA's effect on family caregiver research was published in 2005. Researchers published their experiences in going about research involving family caregivers (adult child, power-of-attorney, etc.). They claimed that due to the IRB being concerned with HIPAA regulations, it added almost a year onto the recruiting process due to them not being allowed to have the contact information of caregivers to send an invite to participate in their study. They instead would have agencies contact the patients giving authorization for them to contact the caregivers and then have agencies contact the caregiver to ask for authorization to receive information from the researchers for a study. To summarize, due to these concerns about

HIPAA regulations, recruitment for studies became much more complicated due to the researchers not being considered covered entities (Albert & Levine, 2005).

Many of the opinions of patients and providers included distrust of how well the policy would work, a low level of understanding of HIPAA and confidentiality, and concern of the difficulties HIPAA would bring to healthcare.

Current Opinions of Patients and Providers on HIPAA and Patient Privacy

Almost 20 years after HIPAA's Privacy Rule was put into effect, many things have changed. HITECH has been in effect for more than ten years now. Now, there are sightly different concerns amongst providers and patients when it comes to HIPAA. There continue to be many data breaches of private health information; this has caused concern and will hopefully lead to changes in the future requiring more strict security measures in protecting patient data online. It is noted that many of these breaches of data could be related to laptops which shows where some of these new security measures should be focused. In addition, with the increase in technology, and social media there are new concerns that will hopefully be addressed in the future within the Privacy Rule in order to keep patient data protected. Some continuing concerns are making certain that the workforce is being trained correctly. Some may say training needs to become more robust as there are still compliance issues to this day (Solove, 2013).

Behavioral Health. Many studies have been done in the past few years looking at the opinion of patients (and providers) on consent, privacy, and HIPAA. One such study was done in a behavioral healthcare facility (Grando et al., 2017). The focus of this study was to learn the opinion patients had on taking granular control (or selective control) of their healthcare, their

opinion on Health Information Exchanges (a network of multiple providers and patient health information within a region or state that allows for easy exchange of health information when it is needed), and their information being used in research. The conclusion of the study was that patients are slightly wishing for selective control of their healthcare information (i.e. disclosing to only certain people and disclosing only certain types of information). It showed that patients were not worried to share information with providers they trusted, and they were more likely to share more information with their behavioral care provider than a specialty doctor. Also, some results of the study showed that patients would benefit greatly from more education on how their personal health information is being used in order for them to make informed decisions on how they would want to control their personal health information, how much they would want to share personal and/or sensitive information with their provider, and if they would want their information shared in an HIE (Health Information Exchange, an online network of providers that allows streamlining of electronic health records and patient information). A few healthcare workers were also surveyed in this study where they gave their opinion on patients having granular control, detailed control of health information such as only allowing some providers access to their information or only access to a certain type of phi. Many thought the option for granular control for patients would be very helpful for the patients because the current process is very broad. However, the caveat was patients would need to be educated by their providers so they could make the best decisions for them if granular control became an option. Things like restricting information on substance abuse could cause issues where the patient would end up having poor quality of care. However, sharing sensitive information like that can also lead to stigma and bias that some patients may be trying to avoid. Overall, providers were interested in

the idea of giving patients granular control, but it would require much more education for the patients than is currently happening. As well, it seems that in order for this education to happen, it needs to be initiated by the provider (which means they would also possibly need more education on HIPAA and privacy) in order for it to be successful.

Youth and Adolescent Care. A different study was done surveying youth from fourteen to twenty-four years old (Zucker et al., 2019). The conclusions of this survey were that many youth patients change how much they share depending on how confident they are that the information would remain confidential. This raises the question of if changes need to be made in billing, treating, or notification policies for treating youth patients if so many of them admit to withholding important or sensitive information from their provider. As well, a large majority of those that responded to the survey could not recall having a discussion with their health care provider about confidentiality at all. A large minority of youth that participated in the survey did not show confidence that their information, especially sensitive information, would remain private. This shows a similarity to the previous study as both youth and behavioral health patients would greatly benefit from receiving more education from their healthcare providers.

Another study was done related to adolescent healthcare, confidentiality, and the use of EHR's (Goldstein et al., 2020). A large cohort of adolescent medicine providers were surveyed on these subjects. It was found that providers were not trained and did not have much in terms of processes on protecting adolescent personal health information on an EHR. Providers felt very comfortable with using EHR's but were highly concerned about the possibility of inappropriate sharing of adolescent health information. This study also focused on the need for EHR vendors to work with the rest of the healthcare system in order to create what is needed in order for

EHR's to remain confidential in the case of adolescents. This would require a large amount of work and cooperation to make an EHR capable of the needs of some adolescents as breaches of confidentiality can occur within multiple areas of the EHR (appointment type, notes, medications, lab orders, etc.). The study also mentioned how creating a perfect EHR would not solve all confidentiality problems for adolescents. Providers must work to keep their patient's information confidential, and insurance billing, a completely separate issue, must also be reworked in order to keep adolescent confidentiality.

Genetic Health. A study of genetic medicine patients was done on their opinion of differences in genetic medicine confidentiality compared to general medicine (Dheensa et al., 2016). Genetic medicine patients were interviewed, and the responses were analyzed thematically. It was found that these patients viewed genetic information such as a mutation to be familial information and should be shared as such. It was found that patients viewed this genetic information to be separate to more personalized information that is commonly viewed as PHI. However, patients also showed concern with understanding how their provider would be treating their information and showed a want for communication with their provider about how their genetic information was going to be treated before faced with a circumstance with family members. These extra moments of discussion appear very helpful for patients and providers, so they are on the same page before addressing family members about test results and mutations. Providers could feel more confident about their communication and patients could have a little bit of control over their information. However, patients also expressed concern with some patients refusing to share their genetic information with family members and felt that perhaps a health care provider should disclose the information anyway. Per HIPAA, disclosing information

like this to family members even when the patient refuses is still allowed due to the possible harm to the family members it may cause if they are not made aware (Security & Privacy Rules, 2002). Another study was done on genetic medicine patients' opinions on their genetic information being personal or familial, and comparing these opinions depending on sociodemographic class, age, and other factors. There were found to be correlations between some of these factors which also show, like the previous study, communication with the patient about how they want their information handled is of the utmost importance (Gilbar et al., 2016).

HIV. A study of HIV patients and their providers was done in order to learn their opinion on if they would feel comfortable sharing their information on an HIE (Maiorana et al., 2012). The patients and providers felt comfortable, overall, with sharing PHI on an HIE. This was based on the foundation of trust between the patients and their providers that was already there, and the comfort patients are gaining with technology. Interestingly, the researchers noted that the communities that this survey was done in had a lot of built-in trust. This seemed to influence the results of the study because the HIV patients truly trusted their providers, the care managers, and the IT staff. Therefore, it shows that patients' comfort level with patient confidentiality and privacy is heavily influenced by their relationship with providers and not the specific policies in place or if their information is in an HIE or not.

Protection of Privacy and not Care. On the other side, some providers in an opinion paper have expressed that HIPAA is causing undue delay in some cases in providing healthcare due to misunderstandings of the Privacy Rule (Berwick & Gaines, 2018). Some unfortunate examples can be the misguided policy hospitals in New Orleans had that caused their workers to not notify family members if their loved one was in their facility after Hurricane Katrina. This

had the possibly to create a very difficult situation and was not protecting patients at all. Many patients had to be evacuated to new hospitals. Those new hospitals originally were not notifying family members if their loved one was in their facility. Thankfully, HHS released a statement reminding hospitals that even without an emergency or disaster, they are allowed to notify family members of a general state of the patient and that they are in their facility (Lyles & Trites, 2005). The writers of the opinion paper claim that due to there not being a contrasting regulation against this undue delay or wrongful refusal to disclose information, organizations feel led to form misguided policies that prevent timely treatment of patients that may need test results or history transferred to a new clinician and but will protect their organization from being penalized by the HHS. In their opinion, these policies have the very big potential to protect the patient's information but not their care (Berwick & Gaines, 2018).

Summary. In general, the opinions and concerns of providers and patients in the present are more nuanced and focused on other things. Patients hear a lot more about HIPAA and read more Notices of Privacy Practices than previously. However, this does not mean patients completely understand HIPAA, confidentiality, or their rights. It seems that no matter the regulations, what always causes patients to feel willing to share health information with their provider, is trust in the provider first, and in the support staff second. Concerns from providers have become more focused on their patients' needs and concerns as providers become more confident in their own HIPAA compliance.

Discussion of Current Confidentiality Issues and Possible Solutions

Misguided Policies

As introduced previously, there are many issues that need to be solved when speaking on confidentiality. Some of those issues include misguided policies or ideas by hospitals, clinicians, and workers that cause harm to their patients. Even after twenty years, there are still issues with healthcare centers/hospitals misinterpreting HIPAA and forming frustrating policies. This shows that more education on HIPAA may not be the solution in this situation. It is proposed the HHS recognize these instances as violations of HIPAA and begin to penalize those that will not disclose to family members if their loved one is in their facility, or they refuse to release patient records to other providers. Under HIPAA, this releasing of records to other providers should not require any new agreement or business associate form; and requiring these extra steps can greatly hurt a patient in need of timely care. Moreover, under HIPAA, a caregiver or loved one should be able to give the name of a patient in a facility, and then receive information about that patient such as if they are in the facility, and an update on the patient's general status. Even if the patient is nonresponsive, HIPAA allows for family members to be generally notified before the patient is able to consent (Security & Privacy Rules, 2002). As can be seen in the new proposed changes to the Privacy Rule, these issues have been noticed and addresses in this new proposed rulemaking. However, these changes are to only clarify what is already in place in the law. Perhaps this will help change the current climate we find ourselves in but in order for real change to happen, these clarifications need to be enforced with threat of penalization if facilities and organizations are not allowing patients their rights under HIPAA or if their policies are causing harm to the patient due to family members being stonewalled or due to refusal to send PHI to other covered entities (Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement, 2021).

Gaps in Policy

Another issue within confidentiality and HIPAA is the existence of businesses that are handling PHI that are not regulated by HIPAA. With the onslaught of new technologies and software, the HHS has been unable to keep up with the changes happening in the world and the noticeable gaps in confidentiality laws and policies are becoming more apparent. Some of the biggest businesses that are causing these policy gaps include wearable technology businesses. The popularity of the Apple Watch and Fitbit have soared to enormous levels and are giving customers valuable information about their health. However, these companies are not required by law under HIPAA to secure and protect their customers' health data. There would only be a requirement if a covered entity or business associate prescribed or provided the wearable technology for a patient (Papandrea, 2019). Other examples of businesses that are handling patient health information without being required to follow HIPAA guidelines include medical record apps and other health apps. Like with Apple Watch or Fitbit, they are only required to follow HIPAA guidelines if the app is having data populated in by a covered entity or business associate. However, if the customer enters the exact same information on their own, there are no HIPAA requirements for that application (Focal Point Insights, 2018). These gaps in protection are very concerning and are spoken about in the article by Papandrea where it is proposed that the best way to close up this gap is to add companies and businesses interacting with a customer's health information onto the Privacy and Security Rule as covered entities (Papandrea, 2019).

Health Information Exchanges (HIE's)

Another current issue in confidentiality and HIPAA is the need for more Health Information Exchanges. These HIE's help to easily transfer information to other providers within an organization, or region. They can streamline services, and help providers have more information to provide the best care possible. The hope is more and more clinics and hospitals will have these HIE's available and use them well. These HIE's would work even better when hospitals and organizations remove any misguided policies that cause delay in sending medical records (Grando et al., 2017; Maiorana et al., 2012). For many years, any legal barriers of using an HIE have been removed. HIPAA has been clarified to allow for sharing amongst other providers. Now, the only issues include getting providers to use HIE's and navigating the differences between state patient consent rules. Possible solutions for getting providers to adopt HIE's include lowering the price or creating a financial incentive to adopt it. As well, different laws are being passed to help with this navigation of state patient consent rules (Mello et al., 2018).

Granular Control

As previously spoken about, granular control of patient health records and privacy is intriguing and would undoubtedly better match the wishes of many patients who would rather share some information and keep other private to only certain providers. The only requirements for granular control to work well would be patient education on how granular control works, what their information is used for, and how their health information benefits them when their providers use it to better prescribe and diagnose (Grando et al., 2017). There are however other things to keep in mind. Some possible effects of granular control can be foreseen due to observations of the GDPR in the European Union. The GDPR requires consumers to opt-in or

consent to anything that is storing their personal data. It has, surprisingly, worked. It is still around and has not been immediately removed. As expected, there have been issues of consumers being overwhelmed by the sheer number of forms and contracts they are constantly receiving in person and online. This has been coined as "consent fatigue" (*The Impact of GDPR One Year Later: The Good, The Bad, and The Future*, 2019; Tovino, 2017). This consent fatigue is something that should be looked out for when considering implementing a form of granular control for patients. As well, these observations of the GDPR show that something like granular control is completely within the realm of possibility.

Explanations of Benefits (EOB's)

A big current issue in patient confidentiality is the complete lack of privacy for dependents when it comes to medical insurance billing. Under the current system of the Affordable Care Act of 2010 and the Employee Retirement Income Security Act of 1974, insurance companies are required to communicate the specific benefits received or denied within EOBs (explanations of benefits) to a policyholder. This is currently completely legal under HIPAA because it involves payment which falls under disclosures that do not require patient knowledge or consent. In the case of dependents such as minors, young adults under twenty-six years, elderly parents/family on the same insurance, and those in an abusive relationship, this possibility of disclosure during an EOB is unsafe or will deter patients from receiving healthcare or even attempting to pay out of pocket for services. Some Title X-funded clinics (Title X provides much stronger protection of confidentiality and privacy within family planning services) will sometimes lower the price or take the full brunt of the payment for patients that require complete confidentiality. This problem of EOB's causing PHI disclosure is trying to be

resolved on the state level because this issue is beyond the scope of HIPAA. The hope is that this problem receives more attention and continues to be looked at on the state level in hopes that new laws be made in order to protect dependents' confidentiality and privacy rights through the entire healthcare process (English & Lewis, 2016).

Education

The final issue that needs to be addressed when speaking about confidentiality and privacy is education. In many of the previous studies mentioned, it was concluded that education for the patient and even the provider would help a great deal (Grando et al., 2017; Zucker et al., 2019). Providers and administrators need to be better educated about HIPAA and privacy in order for them to not misinterpret policies or the law. This is a joint effort that needs to occur in order for the best organization policies to be made on HIPAA. Providers also need to be better educated so they can discuss privacy and confidentiality with their patients in an easy-to-understand and helpful manner instead of using uncomfortable, confusing, and complex jargon that may not translate correctly to the patient. It is even recommended by some that providers stay away from talking about HIPAA and simply make the conversation with their patients using the term, confidentiality (Zucker et al., 2019). This could help patients form a more concrete idea in their mind about their rights and how confidentiality with their provider works.

Before HIPAA was widely in use, many patients still struggled with understanding what confidentiality meant for them. Patients did not have a good idea of how confidential their information could actually be. These issues caused over or under estimation of how protected their health information could be (Sankar et al., 2003). This issue is becoming slightly better over the years, however, now some of these previous issues are being further clouded and dragged

down by overly complicated jargon and information when at the clinic. Instead of hearing about confidentiality, many patients hear only about HIPAA and are given NPP's to sign that give very little useful information to patients that would have been able to help them better understand their rights and how their provider is protecting their PHI. Therefore, the possible changes in place for the Privacy Rule appear very promising and hopefully will change these NPP problems for the better (Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement, 2021).

As previously discussed, the proposed changes to the Privacy Rule include a requirement to change and update the forms patients receive when at the clinic that give their HIPAA policies in order to make them more readable and understandable to the layman (Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement, 2021). Next, patients need to be educated about their rights under HIPAA, how their PHI is being used, and why it is helpful. For instance, many patients without education about HIPAA may overestimate or underestimate how much confidentiality they truly have which was particularly more common in the early implementation of HIPAA (Sankar et al., 2003). So many of these problems surrounding what patients believe about HIPAA and how much they trust the system and are willing to share medical information could be remedied by giving easy-to-understand tools in order to become educated on their rights and also the limits when their information can be disclosed and will not remain confidential. Moreover, patients would greatly benefit from receiving some of this information directly from their provider in order to build trust and rapport. Patients who trust their providers trust them to do the right thing for them when it comes to confidentiality and privacy.

Conclusion

To conclude, HIPAA is a law that has completely changed the way people think about healthcare confidentiality. There have been many modifications and rules added along the way to help identify with the needs of the American people. Now, this is continuing with a new proposed change to the Privacy Rule. As HIPAA has become part of the American healthcare system, providers and patients have given their opinions on these changes and their thoughts on confidentiality.

This review addressed major issues in the United States healthcare system regarding patient confidentiality under HIPAA such as noncompliance amongst providers and healthcare workers, unbalanced privacy regulations by hospital systems and clinics, and lack of education amongst patients. Noncompliance by healthcare workers is still very real and alive even after 25 years of HIPAA regulations (Solove, 2013). The proposed solution to this is a rework/overhaul of the current education system for professionals. Making this education engaging, helpful, and regular (once a year) are important considerations for reworking the current training. The guidelines and recommendations of the HHS are in a constant state of change. Therefore, healthcare workers need to have the resources to understand and apply these new guidelines. As well, because patients will trust their provider with informing them (Grando et al., 2017), the education of healthcare workers should be a top priority so providers and healthcare workers can be equipped to counsel patients on their rights and confidentiality in an approachable, and education-appropriate manner. The unbalanced privacy policies stem from the lack of enforcement by the HHS in regard to misrepresentative policies amongst hospitals (Berwick & Gaines, 2018). A solution to this issue is the HHS creating real consequences for these incorrect

policies that are poorly influencing the experience of patients and their caregivers/families such as a milder version of the current penalties for improper disclosure. One of the most important issues to be resolved when it comes to medical confidentiality is the lack of patient education. Creating resources for patients that are appropriate for age level and their education is extremely important. Having educated patients allows them to set reasonable expectations when it comes to confidentiality and understanding the importance of sharing medical information and history in order to get the best, safest care. The HHS is working to change this education for the better in their new proposed modifications to the Privacy Rule (Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement, 2021) by asking clinics and hospitals to rework the notices of privacy practices to be more beneficial and accessible for the patients. This is very encouraging for the future and is a great foundation to educate patients on privacy. With these three issues addressed, patients, caregivers, family, providers, and healthcare workers will benefit greatly from education, training, and balanced policies.

References

Albert, S. M., & Levine, C. (2005). Family Caregiver Research and the HIPAA Factor. *The Gerontologist*, *45*(4), 432–437.

AMA Council on Ethical and Judicial Affairs. (2012). AMA Code of Medical Ethics' Opinions on Confidentiality of Patient Information. *AMA Journal of Ethics*, *14*(9), 705–707.

Americans With Disabilities Act of 1990, Pub. L. No. 101-336, 104 Stat. 328 (1990).

Berwick, D. M., & Gaines, M. E. (2018). How HIPAA Harms Care, and How to Stop It. *JAMA*, *320*(3), 229–230.

Dheensa, S., Fenwick, A., & Lucassen, A. (2016). 'Is this knowledge mine and nobody else's? I don't feel that.' Patient views about consent, confidentiality and information-sharing in genetic medicine. *Journal of Medical Ethics*, *42*(3), 174–179.

U.S. Department of Health and Human Services. (2021, January 21). HHS Proposes Modifications to the HIPAA Privacy Rule to Empower Patients, Improve Coordinated Care, and Reduce Regulatory Burdens. HHS.gov. https://www.hhs.gov/about/news/2020/12/10/hhs-proposes-modifications-hipaa-privacy-rule-empower-patients-improve-coordinated-care-reduce-regulatory-burdens.html.

English, A., & Lewis, J. (2016). Privacy Protection in Billing and Health Insurance Communications. *AMA Journal of Ethics*, *18*(3), 279–287.

Focal Point Insights. (2018, October 3). *When Does HIPAA Apply to Health Apps?* Focal Point Data Risk. https://blog.focal-point.com/when-does-hipaa-apply-to-health-apps

Gilbar, R., Shalev, S., Spiegel, R., Pras, E., Berkenstadt, M., Sagi, M., Ben-Yehuda, A., Mor, P., Perry, S., Zaccai, T. F., Borochowitz, Z., & Barnoy, S. (2016). Patients' Attitudes

Towards Disclosure of Genetic Test Results to Family Members: The Impact of Patients' Sociodemographic Background and Counseling Experience. *Journal of Genetic Counseling*, *25*(2), 314–324.

Goldstein, R. L., Anoshiravani, A., Svetaz, M. V., & Carlson, J. L. (2020). Providers' Perspectives on Adolescent Confidentiality and the Electronic Health Record: A State of Transition. *Journal of Adolescent Health*, *66*(3), 296–300.

Grando, M. A., Murcko, A., Mahankali, S., Saks, M., Zent, M., Chern, D., Dye, C., Sharp, R., Young, L., Davis, P., Hiestand, M., & Hassanzadeh, N. (2017). A Study to Elicit Behavioral Health Patients' and Providers' Opinions on Health Records Consent. *The Journal of Law, Medicine & Ethics*, *45*(2), 238–259.

Health Insurance Portability and Accountability Act of 1996. Pub. L. No. 104–191, § 264, 110 Stat. 1936 (1996).

Lyles, K. & Trites, P. (2005, December 1). *Lack of medical data, HIPAA no hindrance: Lessons from Hurricane Katrina.* Relias Media. https://www.reliasmedia.com/articles/125087-lack-of-medical-data-hipaa-no-hindrance

Maiorana, A., Steward, W. T., Koester, K. A., Pearson, C., Shade, S. B., Chakravarty, D., & Myers, J. J. (2012). Trust, confidentiality, and the acceptability of sharing HIV-related patient data: Lessons learned from a mixed methods study about Health Information Exchanges. *Implementation Science*, *7*(1), 34.

Mello, M. M., Adler-Milstein, J., Ding, K. L., & Savage, L. (2018). Legal Barriers to the Growth of Health Information Exchange—Boulders or Pebbles? *The Milbank Quarterly*, *96*(1), 110–143.

Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules (informal title: Omnibus HIPAA Final Rule), 45 C.F.R. § 160, 164 (2013). https://www.federalregister.gov/d/2013-01073

News Division of U.S. Department of Health and Human Services. (2021, March 9). *Extension of the Public Comment Period for Proposed Modifications to the HIPAA Privacy Rule*. HHS.gov. https://www.hhs.gov/about/news/2021/03/09/extension-public-comment-period-proposed-modifications-hipaa-privacy-rule.html#:~:text=The%20proposed%20changes%20to%20the,involvement%20in%20the%20care%20of

Office for Civil Rights (OCR). (2009a, September 14). *Breach Notification Rule*. HHS.Gov. https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Office for Civil Rights (OCR). (2009b). *Business Associates*. U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html

Office for Civil Rights (OCR). (2008, May 7). *Enforcement Rule*. HHS.Gov. https://www.hhs.gov/hipaa/for-professionals/special-topics/enforcement-rule/index.html

Office for Civil Rights (OCR). (2009c, September 17). *Security Rule Guidance Material*. U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html?language=es

Office for Civil Rights (OCR). (2008). *Summary of the HIPAA Privacy Rule*. U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

Office for Civil Rights (OCR). (2020, March 26). *HIPAA and COVID-19*. HHS.Gov. https://www.hhs.gov/hipaa/for-professionals/special-topics/hipaa-covid19/index.html

Papandrea, P. (2019). Addressing the HIPAA-potamus Sized Gap in Wearable Technology Regulation. *Minnesota Law Review*, *104*(2), 1095-1132

Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement, 86 F.R. 6446 (proposed January 21, 2021) (to be codified at 45 C.F.R. §160, 164). https://www.federalregister.gov/d/2020-27157

Sabatino, C. (2018, July). *Confidentiality and HIPAA*. Merck Manual Professional Version. https://www.merckmanuals.com/professional/special-subjects/medicolegal-issues/confidentiality-and-hipaa

Sankar, P., Mora, S., Merz, J. F., & Jones, N. L. (2003). Patient Perspectives of Medical Confidentiality. *Journal of General Internal Medicine*, *18*(8), 659–669. 10.1046/j.1525-1497.2003.20823.x

Security and Privacy, 45 C.F.R. § 164 (2002). https://www.govinfo.gov/app/details/CFR-2004-title45-vol1/CFR-2004-title45-vol1-part164

Slutsman, J., Kass, N., Mcgready, J., & Wynia, M. (2005). Health Information, The HIPAA Privacy Rule, And Health Care: What Do Physicians Think? *Health Affairs (Project Hope)*, *24*, 832–842. 10.1377/hlthaff.24.3.832

Solove, D. J. (2013). HIPAA Turns 10: Analyzing the Past, Present, and Future Impact. *Journal of the American Health Information Management Association, 84* (4), 22-28. https://papers.ssrn.com/abstract=2245022

The Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 883. (2008).

The Impact of GDPR One Year Later: The Good, The Bad, and The Future. (2019, May 23). Fair Warning. https://www.fairwarning.com/insights/blog/the-impact-of-gdpr-one-year-later-the-good-the-bad-and-the-future

Tovino, S. A. (2017). The HIPAA Privacy Rule and the EU GDPR: Illustrative Comparisons. *Scholarly Commons at UNLV Law*, *47*, 22.

Vertical timeline. (2020, September 24). https://templates.office.com/en-us/vertical-timeline-tm16400963.

Zucker, N. A., Schmitt, C., DeJonckheere, M. J., Nichols, L. P., Plegue, M. A., & Chang, T. (2019). Confidentiality in the Doctor-Patient Relationship: Perspectives of Youth Ages 14-24 Years. *The Journal of Pediatrics*, *213*, 196–202. 10.1016/j.jpeds.2019.05.056