HIPAA Compliance and the Growth of Telemedicine

Clifton Paul Robinson

Professor Kyle K. Courtney, Esq.

Northeastern University

Khoury College of Computer Sciences

Summer I 2020

Introduction:

As we move forward into the age of technology the focus has shifted towards making devices and software that are convenient for the consumer. In just the past decade we have seen a boom in convenient technology such as the Internet of Things devices, auto-driving cars, and tablet computers.[1] The technological boom does not only focus on the everyday consumer, other fields, such as healthcare and agriculture, have benefitted immensely over the last decade.

The healthcare industry is continuously developing and evolving to work best for the patients. Several key advancements in healthcare are the electronic health record, that allows patients information to be easily shared, wearable technology that lets people with health concerns be monitored more easily, and telemedicine, that allows patients to have online meetings with a physician from the comfort of their own home.[2] Unlike regular consumer products, companies cannot just create and roll out new healthcare products without adhering to stricter guidelines. They also need to comply with the Health Insurance Portability and Accountability Act, HIPAA for short.

HIPAA was signed by President Bill Clinton in 1996 with several key components to it. The primary goals are to (1) modernize the flow of healthcare information, (2) specify how Personally Identifiable Information (PII)[3] is kept by the healthcare industries so it is protected from theft and fraud, and (3) address the limitations on healthcare insurance coverage.[4] This landmark act added multiple safeguards to healthcare patients by holding healthcare providers, health plans, healthcare clearinghouses, and business associates of HIPAA-covered entities to implement protections for sensitive personal and health information.

Now, this seems like an act that does not actually need to be implemented, why would any healthcare organization want to have sensitive data stolen? The short answer is none. The need for HIPAA goes beyond the protection of this data, it is about accountability. Without HIPAA, there would be no requirements for these organizations to add safeguards to data as well

---

[1] Ryan, K. (2019, December 16). The 10 Greatest Inventions of the Past Decade. Retrieved June 18, 2020, from https://www.inc.com/kevin-j-ryan/greatest-inventions-decade-2010-2019.html

[2] 10 Biggest Technological Advancements for Healthcare in the Last Decade. (n.d.). Retrieved June 18, 2020, from link.

[3] Personally Identifiable Information is any information that can be used to identify the person.

[4] United States. (2004). The Health Insurance Portability and Accountability Act (HIPAA). Washington, D.C.: U.S. Dept. of Labor, Employee Benefits Security Administration.

as no repercussions if they failed to implement them. On top of that, it requires that "healthcare organizations control who has access to health data, restricting who can view health information and who that information can be shared with," as well as how data is transmitted, stored, and the security controls needed to protect it.[5] This is why we have a need for HIPAA, especially today with the technology being created for healthcare. Accountability is everything when it comes to private data and that is one key aspect of this act.

Creating HIPAA compliant technology is not always easy and that is especially true when it comes to telemedicine.[6] Telemedicine is not a new concept, it started in the 1950's when several hospital systems and university medical centers started sharing information over the telephone. Over the next several decades this was a popular option, especially in more rural areas, because remote visits were still expensive.[7] With the expansion of the internet, telemedicine has evolved to become even more convenient for both doctors and patients. With the advancement of high-quality video transmission, it allows for easier communication and quicker ways for patients and their doctors to communicate.

There is currently a need for telemedicine as well as the correct resources to deploy it nationwide. However, it is not as simple as just creating a healthcare video communication system, there is also the need to keep these systems HIPAA compliant. In these online appointments, they will be discussing information that is covered under HIPAA in real time. This means that the entirety of this communication must be secure so there is no way that this information will get hacked or stolen.

By looking at specific HIPAA complaints and court cases we can understand the path telemedicine will take moving forward. It is also important to look at the current events of today, due to the COVID-19 (coronavirus) Pandemic there has been an even more important need for telemedicine. However, due to the rush, the Office for Civil Rights (OCR) has waived certain HIPAA Liability on Telehealth. Through all of the sources, the impact and use of telemedicine will become more clear.

---

[5] Alder, S. (2019, February 20). Why is HIPAA Important? Retrieved June 18, 2020, from https://www.hipaajournal.com/why-is-hipaa-important/

[6] Telemedicine is a subsection of Telehealth that specifically focuses on electronic communications and software to provide clinical services to patients.

[7] What is Telemedicine? (n.d.). Retrieved June 18, 2020, from https://chironhealth.com/telemedicine/

Telemedicine: The Need and the Legal Issues

Telemedicine seems to be a step in the right direction for a new age of healthcare options. It is growing rapidly, being a $17.8 billion industry and growing roughly 18% annually over the past five years.[8] There is also a growing need for these types of consultations, as many patients need the convenience and accessibility that this option provides them. Telemedicine works like a business and for it to continue being successful convenient for both the patient and the doctor is key. Common complaints about going to the doctors consist of the wait times and the amount of time they actually see the doctor to name a few. Telemedicine eliminates both of these issues as well as offers the patients a way to see a doctor quickly and without much turnaround time.

Time is not the only form of convenience though, availability is also crucial. It was reported that for every 100,000 rural patients, there are only 43 specialists available.[9] The lack of specialists in these rural areas creates scheduling issues where they cannot see every patient who needs to be seen within a respectable time. Telemedicine fixes this issue. Doctors can refer their patient to the specific physicians they need, regardless of location. It has also been shown that telemedicine patients score lower for depression, anxiety, and stress, and have 38% fewer hospital admissions.[10] Thus having many positive improvements on a patients day-to-day life.

This option does not come without drawbacks though. There are several major legal issues that still seem to be unclear as this industry grows. One common issue is that these appointments can take place anywhere. A doctor in Massachusetts could be on a call with a patient in Oklahoma. This means that the doctor has their medical licence to only practice in Massachusetts. For them to conduct the appointment they would need to secure a license from the client's state unless the state has exemption provisions.[11] This is a significant legal issue as well as a confusing one. Organizations that are using this industry will need to stay on top of the current laws as well as the locations of everyone involved to make sure there is no malpractice.

---

[8] Telemedicine Benefits and Disadvantages, Telemedicine Pros and Cons. (2020, January 01). Retrieved June 19, 2020, from https://evisit.com/resources/10-pros-and-cons-of-telemedicine/

[9] Hing, E, Hsiao, C. US Department of Health and Human Services. State Variability in Supply of Office-based Primary Care Providers: United States 2012.

[10] Pande, R. L., Morris, M., Peters, A., Spettell, C. M., Feifer, R., & Gillis, W. (2015). Leveraging remote behavioral health interventions to improve medical outcomes and reduce costs. The American journal of managed care, 21(2).

[11] Cason, J., & Brannon, J. A. (2011). Telehealth regulatory and legal considerations: frequently asked questions. International journal of telerehabilitation, 3(2), 15–18. https://doi.org/10.5195/ijt.2011.6077

Another crucial issue is that states have different laws concerning if and how telehealth can occur. This stems from the fact that there has been inconsistent adoption of laws regarding the use of telehealth with two examples being the American Speech-Language-Hearing Association (ASHA) and the Federation of State Boards of Physical Therapy (FSBPT) recommended laws and policies.[12] States have cherry-picked the parts they want to implement while ignoring other parts. To start practicing, it is extremely important to check a state's statutes, regulations, and policies before starting to practice. This adds another area where an organization should be well versed in states laws to practice legally.

A third legal issue is how states allow telemedicine to be conducted. There are ways that may not allow the practice or create barriers for its use. An example of this can be seen in Delaware for speech-language pathology and audiology, where a regulation states "Licensees shall not evaluate or treat a client with speech, language or hearing disorders solely by correspondence. Correspondence includes telecommunications".[13] This means the use of telemedicine within their state for speech-language pathologists and audiologists is significantly limited by defining telecommunication this way. As well as poor wording, some states do not even mention telehealth, this means that practitioners need to contact the state board for clarification to ensure that they do not violate any part of their license.[14]

The last major legal issue is about professional malpractice insurance. Before starting this practice, practitioners need to consult with their malpractice insurance carrier to ensure telemedicine is covered within their plan. This occurs a case-by-case basis, some carriers allow it and some do not. It also gets even more complicated if the practitioner plans to practice across multiple states. Adding another layer that could possibly halt practicing in this form.

While doctors and patients are ready for widespread use of telemedicine, most states are not. The issues that are plaguing the advancement of this come from outdated or vague laws on a state level. To help fix these legal issues, states will need to focus on implementing similar laws

[12] Pande, R. L., Morris, M., Peters, A., Spettell, C. M., Feifer, R., & Gillis, W. (2015). Leveraging remote behavioral health interventions to improve medical outcomes and reduce costs. The American journal of managed care, 21(2).
[13] Delaware General Assembly Title 24 Professional Regulation, 2006, Section 9.2.1.4
[14] Pande, R. L., Morris, M., Peters, A., Spettell, C. M., Feifer, R., & Gillis, W. (2015). Leveraging remote behavioral health interventions to improve medical outcomes and reduce costs. The American journal of managed care, 21(2).

that mirror other states or the Federal government will need to step in to help. Even with these issues, telemedicine will continue to push on.

HIPAA and Telemedicine:

For telemedicine systems to be compliant with HIPAA the focus needs to be shifted to the safety of electronic protected health information (ePHI). Outside of general HIPAA compliance, they have released guidelines for telemedicine:[15]

- Only authorized users should have access to ePHI.

This bullet point is straightforward. For this rule to be met, physicians just need to make sure that they use "reasonable and appropriate safeguards" to make sure no ePHI has been disclosed to any unauthorized users or parties.

- A system of secure communication should be implemented to protect the integrity of ePHI.

This bullet point is more specific. This means that an insecure communication channel ***cannot*** be used for communicating ePHI. This includes applications such as SMS, Skype, and email. The reason these will not be sufficient is because they store the data as well meaning there would need to be a Business Associate Agreement (BAA) with the third party storing the data. This is to ensure the protection of the ePHI and provisions for regular auditing of the data's security. To give an example, Verizon, Skype and Google will not enter into BAAs with covered entities for these services because they lack HIPAA-compliant security measures.

- A system of monitoring communications containing ePHI should be implemented to prevent accidental or malicious breaches.

This means that any system communicating ePHI over a network must be able to monitor and remotely delete anything if necessary. This also requires mechanisms that do not leave the system vulnerable if there is a long period of no use.

When it comes to compliance requirements, the HIPAA guidelines do not ask these healthcare organizations to reinvent the wheel when it comes to telemedicine. For many of these organizations, they have been "pleasantly surprised" by the ease of complying with these

[15] HIPAA Guidelines on Telemedicine. (2020, May 19). Retrieved June 19, 2020, from https://www.hipaajournal.com/hipaa-guidelines-on-telemedicine/

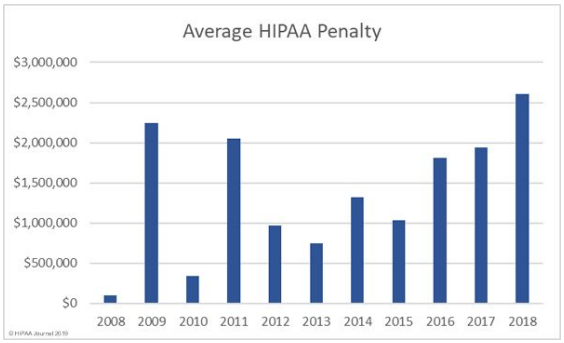
guidelines as well as the price for utilizing this method.[16] There are three points in particular that these organizations have mentioned that make compliance easier:

1. No need to invest in expensive hardware,
2. The software is not complicated, and
3. The system does not drain the organization's IT resources.

As these systems become more advanced, compliance will probably come intact with the system.

HIPAA Complaints and Cases:

While compliance is easy to achieve, it is not always followed. In 2018, the average financial penalty for a HIPAA violation was $2,607,582 with a total of $28,683,400 being paid to the OCR.[17] To understand the impact of HIPAA and the violations it helps to look at several of the most important violations since its creation as well as ones that are based on telemedicine. From this, a pattern can be seen for the major issues with becoming HIPAA compliant. By understanding the essence of these violations, healthcare organizations can focus on ways to strengthen their weaker areas. To understand what the Department of Health and Human Services (HHS) looks for, the list of the most common violations helps:[18]



Unsecured Records	Unencrypted Data	Hacking	Loss of Devices	Lack of Training
Gossiping / Sharing PHI	Employee Dishonesty	Improper Disposal of Records	Unauthorized Information Release	3rd Party Disclosure of PHI

It is also interesting to note that half of these violations are due to human error, better known as insider threats, whether malicious or negligent.

[16] HIPAA Guidelines on Telemedicine. (2020, May 19). Retrieved June 19, 2020, from https://www.hipaajournal.com/hipaa-guidelines-on-telemedicine/
[17] Adler, S. (2019, February 08). Summary of 2018 HIPAA Fines and Settlements. Retrieved June 19, 2020, from https://www.hipaajournal.com/summary-2018-hipaa-fines-and-settlements/ (Also for the graph)
[18] Houseman, K. (2016, December 03). Top 10 Most Common HIPAA Violations. Retrieved June 20, 2020, from https://www.revelemd.com/blog/top-10-most-common-hipaa-violations

The first violation will be the one from 2013 against Advocate Health System, a company in Illinois. The issue started when four laptops were stolen from an Advocate office that contained information on over 2,000 patients, potentially compromising them all. Something similar happened later that year when a laptop was then stolen from an employee's vehicle, compromising more patients. The OCR conducted an investigation and discovered that the company had not assessed any of the risks of its ePHI, restricted physical access to their IT systems, nor received any written record that employees would protect the ePHI and guard an unencrypted laptop while it was in an unlocked car.[19] Advocate Health Care agreed to pay $5.55 million to the HHS' Office for Civil Rights to settle the claims that it violated. The director of OCR at the time, Jocelyn Samuels, said "we hope this settlement sends a strong message to covered entities that they must engage in a comprehensive risk analysis and risk management to ensure that individuals' ePHI is secure".

This fine is still the largest amount to date for HIPAA violations. This case can also be applied to telemedicine as well. For this system to work, practitioners need a laptop to connect, whether it be a personal or provided one. In either case, there can easily be a failure to encrypt the laptop or protect the ePHI that is stored on it. To stay compliant, it is crucial to stay up-to-date on risk factors posed to any of the IT systems. A laptop that can connect to the communication system must be properly secured and the right steps must be taken to also encrypt the data.

The second general violation was against the Advanced Care Hospitalists PL (ACH) in 2018. ACH started using a billing data processing service between November 2011 and June 2012 from an individual who pretended to be a representative of Doctor's First Choice Billings, Inc. (First Choice), a third party billing company. ACH never entered into a business associate agreement (BAA) with the third party billing company. It turned out that the individual was using First Choice's name and website without any knowledge or permission. In 2014, it was made aware that ePHI and other sensitive information of patients was viewable on First Choice's website. When OCR investigated this complaint it revealed that ACH failed to:

1. Enter into a BAA with the individual who purported to work on behalf of First Choice;

[19] Resolution Agreement and Corrective Action Plan between OCR and Advocate Health Care Network

2. Enter into a services agreement with the individual who purported to work on behalf of First Choice;
3. Implement any HIPAA Privacy, Security, or Breach Notification rule policies or procedures until April 1, 2014; and
4. Conduct a risk analysis until March 4, 2014.

This led to possibly 9,000 individuals being compromised and ACH paying a $500,000 settlement.[20]

While this is a basic HIPAA violation it still plays a direct role into telemedicine compliance. Earlier it was stated that third-parties must enter a BAA with the organization. The reason it is important to enter a BAA is because it is used to to maintain PHI security and overall HIPAA compliance between the organization and the third-party.[21] For these systems to be put into place a third-party is still needed, which means a BAA is also. For these healthcare organizations, investing in their own private telemedicine infrastructure would be a major investment that would pay off in the long run. The downside is, these systems would require a decent amount of money and a whole team of developers at the least. This makes entering into BAA's a top priority in this field.

The third and final violation is one that ties into telemedicine through the actual violation. In 2016, HHS settled a case with the Phoenix Cardiac Surgery for a lack of HIPAA safeguards. This violation happened because the surgeons were posting their surgical and clinical appointments on a public, internet-accessed calendar that anyone could view. This is one of the most basic violations that can be caused. On top of that, they had implemented only a few policies and procedures to comply with the HIPAA Privacy and Security Rules, and had limited safeguards in place to protect patients' electronic health information (ePHI).[22]

This ties directly into telemedicine. It actually violates the first two points of telemedicine HIPAA compliance. While this does not handle the communication between surgeon and patient, it is still a form of communication that contains ePHI over the internet. The necessary safeguards are needed on multiple levels for this system to be implemented safely and securely. In this case,

[20] Advanced Care Hospitalists PL (ACH) No-Fault Settlement and Two Year Corrective Action Plan (CAP)
[21] Snell, E. (2017, April 28). What is a HIPAA Business Associate Agreement (BAA)? Retrieved June 20, 2020, from https://healthitsecurity.com/features/what-is-a-hipaa-business-associate-agreement-baa
[22] Phoenix Cardiac Surgery Resolution Agreement

an error can affect the entire operation, but this could also happen on an end-to-end communication software.

It is hard to understand the exact violations that telemedicine faces because there are not any. A lot of these HIPAA cases end up being basic violations because even when they violate more specific areas, it also violates the core ideals of the act itself. However, there was a major court case in Texas that has helped shape telemedicine currently. By looking at these cases, a general understanding can be formed about how the courts see this technology and the direction it will take.

In 2015, Teladoc, a national telemedicine provider in Texas, filed a complaint calling on the Court to prevent the Texas Medical Board from putting into effect a new rule that would require physicians to have face-to-face encounters with new patients prior to writing prescriptions.[23] This law would have quickly put Teladoc out of business because in 2014, their operations in Texas generated $10 million, which was roughly a quarter of the company's total yearly revenue.[24] Two years later, Teladoc dropped their lawsuit because the Texas governor signed the telemedicine laws, which allowed Teladoc to expand its offerings in the state as well as removing the face-to-face requirement.[25]

Even at a state level, this case is an important win for telemedicine across the board. Many of these companies are 100% online, never requiring a real face-to-face conversation. Teladoc saw that their company would go bankrupt from a short-sighted bill and fought for their rights and won. Short-sightedness has played a role in limited telemedicine, just go back to the example about Delaware. These companies will need to be focused on specific wording in these new bills to make sure they are not put at a disadvantage.

COVID-19's Impact on Telemedicine

The impact of the coronavirus is worldwide with basically everything shutdown. With all of the concerns around public health, telemedicine has been forced into centerstage. This has

[23] 22 Tex. Admin. Code § 190.8
[24] Murphy, K., PhD. (2015, June 02). Legal Case to Impact Future of Telehealth Services in Texas. Retrieved June 20, 2020, from https://mhealthintelligence.com/news/legal-case-to-impact-future-of-telehealth-services-in-texas
[25] Davis, J. (2017, December 04). Teladoc drops Texas lawsuit as state adopts new telemedicine regulation. Retrieved June 20, 2020, from link.

actually led to a limited HIPAA waiver. This has happened because when a public health emergency is declared, the Secretary of the HHS may choose to waive certain sanctions and penalties for noncompliance with specific provisions of the HIPAA Privacy Rule. This waiver covers five provisions from the HIPAA Privacy Rule, which are:[26]

- The requirements to obtain a patient's agreement to speak with family members or friends involved in the patient's care – 45 CFR 164.510(b)
- The requirement to honor a request to opt out of the facility directory – 45 CFR 164.510(a)
- The requirement to distribute a notice of privacy practices – 45 CFR 164.520
- The patient's right to request privacy restrictions – 45 CFR 164.522(a)
- The patient's right to request confidential communications – 45 CFR 164.522(b)

It is also important to note that the HIPAA waiver only applies in areas covered by the public health emergency. This waiver has made it easier for healthcare practitioners to utilize telemedicine while keeping patients safe and healthy.

This is a well put together waiver that covers multiple areas to avoid abuse or wrongdoing. Overall, this is putting necessary provisions into place to help aid in the fight against coronavirus. There is a reason this power exists when a public health emergency is declared, certain privacy rules are not needed during this time if it can dramatically impact the effort in a positive way.

Moving Forward with Telemedicine

When asking what comes next for this area there are multiple directions that can be taken. The first step will be improving the communication. While these systems work well, there is still a need for improved systems that do not drop audio or video while a session is happening.[27] This also leads into hospitals and health centers implementing these services as well. Allowing patients to see their primary care doctor or specialist without an in-person visit can be beneficial

[26] Limited Waiver of HIPAA Sanctions and Penalties During a Nationwide Public Health Emergency

[27] Telemedicine Benefits and Disadvantages, Telemedicine Pros and Cons. (2020, January 01). Retrieved June 19, 2020, from https://evisit.com/resources/10-pros-and-cons-of-telemedicine/

for both parties and create a better sense of trust and understanding between the two. In the short term, these are easy solutions that will create a stronger base for telemedicine.

As this technology continues to advance, it brings more conversations into the fold. Under Article 25 of the United Nations' 1948 Universal Declaration of Human Rights states that "Everyone has the right to a standard of living adequate for the health and well-being of himself and of his family, including food, clothing, housing and medical care and necessary social services." By making telemedicine a common option in the United States citizens can gain access to comprehensive and quality health care services that are important for maintaining health, preventing and managing disease, reducing unnecessary disability and premature death, as well as achieving health equity for all.[28] While this does not solve all of the problems that are posed by healthcare, it is a strong first step towards providing healthcare as a basic human right.

Lastly, there needs to be a focus on cyber-healthcare infrastructure. While there is an answer in third-party companies, the healthcare organization always tied in with a BAA. By creating a separate infrastructure that is only used for telemedicine. A safety net is created that allows for a single location for all of this to take place. This type of infrastructure would be created to already be 100% HIPAA compatible and allow easy setup for anyone in this field to use. If telemedicine can evolve to a single critical infrastructure network it will make complying with HIPAA second nature.

Conclusion

Whether it was ready or not, telemedicine has taken a crucial role over the last several months due to the pandemic. Having a service that can expand access to essential health services with a click of a button was needed to stay on top of everything.[29] As the healthcare industry evolves from this pandemic there will be a focus placed onto telemedicine and making it more readily available, which means it has to be ready. To do this, the healthcare industry and the government will need to work together to put laws into place to allow a seamless transition into an age of telemedicine.

---

[28] Health Equity Brief Access to Health Care in Allegheny County

[29] Using Telehealth to Expand Access to Essential Health Services during the COVID-19 Pandemic. (2020, June 10). Retrieved June 20, 2020, from https://www.cdc.gov/coronavirus/2019-ncov/hcp/telehealth.html

There needs to be a focus put onto HIPAA compliance within this area. While there are guidelines on staying compliant, most of these major cases have stemmed from basic violations. It is also important to look at current laws that may have been shortsighted and hinder the growth of this area. By continuously looking, learning, and correcting past mistakes there can be a better tomorrow. While telemedicine continues to evolve into a new form of healthcare, there is a need to continue building off of it to let it become a more secure way to healthcare, privacy, and equality.