HIPAA in the Digital Age:
Redefining existing legislation to protect virtual healthcare providers & patient information online.

Anthony Dellocono, Luke Hendriksen, Alec Macartney

Andrew Gard, PhD

Executive Summary

Privacy concerns were limited to the physical invasion of homes and personal conversations; however, with increased access to digital tools, individuals are concerned about the security of their data online. The rapid digitization of healthcare presents a plethora of health data without protection under current regulation. The closest American's get to protection under the law of their health is the Health Insurance Portability and Accountability Act of 1996 (HIPAA) – a law signed because of insurance concerns.

Our proposal, HIPAA in the Digital Age, uses the original insurance framework of HIPAA to protect patient data from the greatest privacy threat online, data brokers. HIPAA today only applies to "covered entities," a term associated with health insurance. One defined covered entity, health care clearing houses, is ripe for expansion to data brokerages.

Our proposal expands the definition of healthcare clearinghouses to include data collected through *"the network of internet-connected devices, hardware infrastructure, and software applications used to connect health information technology."* By including these streams of data in HIPAA, those collecting this valuable data will be subject to the law's privacy and security rules and unable to sell patient data (FTC). These small changes to an outdated law will keep more information private, limit the information available to data brokers, and hold virtual healthcare to the standards of its predecessors.

Policy Benefits

While expanding any existing federal legislation bears risks, ensuring that the private health information of Americans is safe in a digital age offers several advantages:

1. Patients can trust online service providers, peer health communities, online health management tools, and virtual research surveys with private health data.
2. Health professionals can securely leverage the power of the data and the internet to optimize patient outcomes uniformly across the United States.
3. Data brokers are unable to exploit patient health information for profit.
4. Consumers and counsels are provided a legal framework is provided for violations of health data privacy online.

Proven Success

Several policies have responded to similar concerns about data privacy on the internet. In 2018, the Colorado Privacy Act (CPA) became the most stringent measure of consumer data privacy protection. The act takes a similar approach to our proposal by changing the definition of *covered entity* to mean any organization or person "who maintains, owns, or licenses personal identifying information of an individual residing in Colorado" (Peters). The CPA's broad definition has led to solutions like ours, but the benefits are undeniable:

- Increased notification of data breaches to government officials and residents
- Better tracking of patient data being collected and how it is used thereafter.
- Penalties for misuse of health data and violation of patient rights.

Scope and Operations

Our proposal would hold any entity collecting data from "the internet of medical things" to the standards of HIPAA and its regulatory bodies (FTC). These entities include but are not limited to: social media platforms, health tracking apps, and wearable technology. The cost of adherence is on the companies behind products like these and the motivation of adherence is the threat of enforcement. The penalties and cost of enforcement of HIPAA still default to the Department of Health and Human Services (HHS) under this proposal, with expanded legal precedent for interventions by the Federal Trade Commission (FTC). The success of these

operations will be evident in increased privacy interventions by regulatory bodies and consumer privacy cases citing new HIPAA definitions in the courts.

Table of Contents

Introduction

Lawmakers are at a crossroads when it comes to regulating big data, especially data that pertains to consumer health. The RBC Capital Market projects that "by 2025, the compound annual growth rate of data for healthcare will reach 36%" based on estimates in 2017 ("The Healthcare Data Explosion"). This projection puts the growth of healthcare data ahead of manufacturing, financial services, media, and entertainment. A similar 2018 estimate by Statista projected 2,314 exabytes of new health data could be generated in 2020 (Stewart). To put the sheer mass of this data into perspective, a gigabyte is a size of Earth and an exabyte the size of the sun, although the impacts of the COVID-19 pandemic and the shift from in-person to online healthcare are not reflected in these projections. What has been called the "healthcare's data tsunami" is the inflection point of the healthcare industry's digital transformation exacerbated by a pandemic (Hoey). Similarly, these projections do not take into consideration the health data that is collected by entities outside the healthcare system, such as websites, apps, and smart watches.

However, health data provides consumers with many risks in addition to its opportunities. Health information is intrinsically personal, making it ripe for privacy concerns. These concerns have called into question the lack of federal legislation considering safe storage, proper use, transparent collection, and the sale of such sensitive information. Legislators are stuck in the vast and dynamic landscape of health data, navigating comprehensive regulation without sacrificing optimization.

Digital Landscape of Health Data

Before delving into the health data privacy issues mentioned above, it is important to look at the current impact the digital landscape has had on health data and its collection.

Technological increases have paved the way for the market of digital healthcare to demonstrate significant growth in recent years as well. According to a report by Grand View Research, the global digital health market size was valued at USD 211.0 billion in 2022 and is expected to grow at a compound annual growth rate of 18.6% from 2023 to 2030 (Grand View Research). This growth rate is incredible, and as already noted, can have both positive and negative impacts on the general populace.

One of the major factors driving the growth of the digital healthcare market is the increasing prevalence of chronic diseases, which account for a large portion of healthcare spending worldwide (Klein). Digital health technologies such as remote patient monitoring, telemedicine, and mobile health apps have the potential to improve the management of chronic conditions and reduce healthcare costs (Klein). Another factor contributing to the growth of the digital healthcare market is the widespread adoption of electronic health records, or EHRs for short, which provide a centralized source of patient information that can be easily accessed and shared among healthcare providers (GVR). In fact, the global electronic health records market size has also been valued at USD 27.2 billion in 2021 and is also expected to grow at a compound growth rate of about 4.0% from 2022 to 2030 (GVR).

Overall, the digital healthcare market is expected to continue its rapid growth in the coming years. The increasing demand for digital health technologies is caused partly due to mobile health apps and the widespread adoption of EHRs, which is why it is essential that these entities are given the same protection security as traditional health entities.

New Technology

The increasing use of electronic health records, wearable devices, and mobile apps is transforming the way healthcare is delivered and managed. With this transformation comes new

opportunities for improving patient outcomes, reducing costs, and enhancing the overall quality of care (DHHS). The digital landscape of health data also presents a vast amount of information that can be used to inform medical decisions, support research, and improve public health (DHHS). Electronic health records, for instance, provide a comprehensive and centralized source of patient information, which can be easily accessed and shared among healthcare providers. Wearable devices can collect real-time data on patient activity levels, vital signs, and other health indicators, providing valuable insights into patient health and behavior (DHHS). Overall, health data today is much easier accessible by a multitude of providers, leaving it a vulnerable target.

Emerging Threats

However, with the new digital transformations comes significant challenges that must be addressed. One major concern is ensuring the privacy and security of health data. As health information is increasingly collected and shared electronically, it is crucial to establish robust safeguards to protect against individual identifiable health information (DHHS). One threat against secure personal health information is uncertainty around data ownership and access, which raises questions on how health data can be used ethically and responsibly (World Health Organization). Another major problem regarding unprotected personal health information is its use in marketing techniques. Because of the lack of a federal privacy safeguard, identifiable health information is up for grabs by third parties looking to exploit individuals for profit. The Department of Health and Human Services identified “conflicts of interest, such as ties to the pharmaceutical industry, which were not disclosed to individuals using these sites” (DHHS). One final threat of unprotected online health data is the vulnerability to data breaches. Non covered entities are not mandated to protect health data “with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to

prevent unauthorized or inappropriate access, use, or disclosure", in the same way that covered entities are required by HIPAA. Ultimately, more needs to be done about the current standard of health data protections, which leaves the consumer's identifiable health information an easy target for breaches, marketing, and questions of ownership.

Current State of Regulation

In response to the growth of technology and potential data privacy risks, a handful of states in the U.S. have acted and created their own privacy laws to make up for the lack of federal regulation. California and Colorado specifically have very strong privacy laws in place. The California Consumer Privacy Act, or CCPA for short went into effect on January 1, 2020, (California Office of the Attorney General, with the primary goal being to give Californians more control over their personal information (OAG). Under the CCPA, Californians have the right to know their personal information being collected, the right to request deletion, and the right to opt-out of the sale of their personal information (OAG). Businesses must also provide clear and conspicuous notices to California residents about their data collection and processing practices. The CCPA also requires businesses to implement certain data security measures to protect personal data and it imposes fines and penalties for non-compliance, with penalties ranging from $2,500 to $7,500 per violation (OAG).

The Colorado Privacy Act, otherwise known as CPA, went into effect in July of 2021, providing the right to opt out of the sale of personal data, certain types of profiling, and targeted advertising to Colorado residents. In addition, they have the right to access and even delete their personal data altogether. The CPA also defines the term "sensitive data," which is a pertinent term for our topic, stating that it includes "personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation,

citizenship or citizenship status, genetic or biometric data that may be processed for the purpose of uniquely identifying an individual, and the personal data of a known child" (Husch Blackwell). Businesses are not allowed to process sensitive data without the explicit consent of the consumer. The last important protection that the CPA provides is the restriction of data collection, requiring that the specific reason for the data collection be "adequate, relevant, and limited to what is reasonably necessary in relation to the specified purposes for which the data is processed" (Husch Blackwell). Lastly, the CPA requires controllers to properly secure the personal data that has been consented upon.

Although these two laws are incredibly strong and would help solve some of the issues plaguing data privacy, they only protect certain regions of the United States. Implementing a comprehensive federal policy addressing data privacy would benefit the entire with the protection of private information. This is the intent of expanding HIPAA to cover mobile health technology. With the influence of the California and Colorado state laws, an amendment to the main foundation of private medical information secures both traditional and electronic data for everyone in the United States. HIPAA has been successful in limiting the disclosure and sale of identifiable health information since its enforcement, which is why its expansion is the best possible route for providing protection for each American.

Background of HIPAA

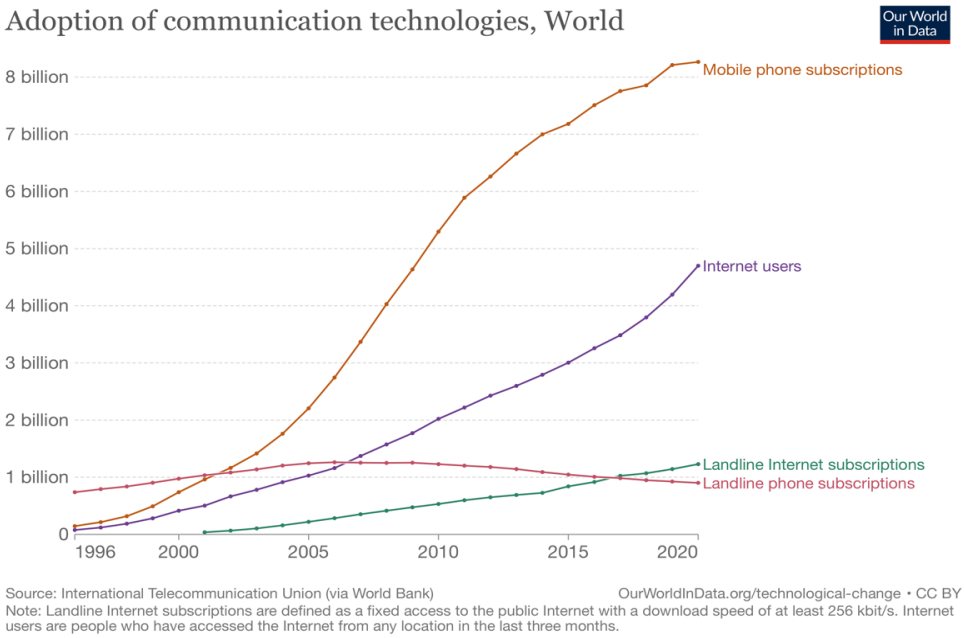
The solution we identified as most likely being the most efficient for this problem is to approach it from the federal level and expand HIPAA. HIPAA's privacy rule was designed to address the use and disclosure of individuals' health information, and it contains standards for individuals' rights to understand and control how their health information is used (Center for Disease Control and Prevention). For clarification, HIPAA's privacy rule protects individually

identifiable health information, which is " data that relates to: the individual's past present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual" (HHS). However, the current privacy rule does not extend to all health-related entities, but rather only ones designated as covered. A covered entity, as defined by HIPAA, is any type of traditional healthcare provider, health plan, healthcare clearinghouse, or business associate (CDC). The permitted uses or disclosures of personal health information via these entities are for the following situations: "disclosure to the individual, treatment, payment, and healthcare operations, incident to an otherwise permitted use and disclosure, limited dataset for research, public health, or healthcare operations, and public interest and benefit activities" (CDC).

HIPAA also has a security rule along with its privacy rule, which covers the same entities as the privacy rule, but for electronic personal health information. This rule stipulates that covered entities must ensure the confidentiality and availability of all electronic personal health information, safeguard against anticipated threats to the security of this information, protect against illegal uses or disclosures, and ensure the compliance of its workforce (CDC). The privacy and security rules establish clear boundaries for health data collected by traditional stakeholders in the healthcare system, such as doctors, nurses, hospitals, and clinics. However, new stakeholders in the industry are finding ways around HIPAA's boundaries using technology to collect health data.

HIPAA was originally created in 1996 and has seen five additions since its enforcement (HIPAA Journal). These include the privacy rule added in 2003, the security rule in 2005, the

breach enforcement rule in 2006, the breach notification rule in 2009, and the final omnibus rule in 2013 (HIPAA Journal). Since 2013, there have been no further additions or amendments to the law, and it has become increasingly evident that the legislation is outdated. Below is a graph highlighting HIPAA's obvious need to be upgraded and expanded.



(Fg. 3 "Technological Change." Our World in Data)

According to the graph, mobile devices and the internet's usage has drastically increased between the time when HIPAA was created and 2020. As usage and demand increases, technology tends to follow suite and evolve accordingly. The capabilities of technology are continuously expanding, which inherently means that how data is collected, processed, and sold do as well. While technology has changed dramatically within the past twenty-seven years, HIPAA has remained relatively constant since its creation with only minor adaptations. It is because of its stagnation that an amendment to HIPAA is strongly recommended.

The Issue at Hand

Largely ignored in privacy legislation, data brokers are ignored for bigger targets like social media companies and their artificial intelligence algorithms despite posing a unique threat to private health data (Sherman). Without regulation, data brokerages or companies buying and selling data on consumers "sell billions of sensitive data records for various purposes" without government oversight or tracking (Kim). These companies can buy or sell an individual's health data for any purpose without consent or repercussions.

Only two laws on the books define data brokers and brokerages: California's Civil Code § 1798.99.80 and Vermont's Statute 9 V.S.A. § 2430. Legislators in California took a step towards regulation with the civil code by requiring data brokers to register as "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship" ("Section 1798.99.80 - Definitions, Cal. Civ. Code § 1798.99.80."). Vermont followed suit by mandating data brokerage disclosure to the state as "a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship" ("Vermont Laws."). In both cases, exemptions are made, which weakens already loose definitions. For example, Facebook would not be considered a data broker if it sold user information under California's definition because the company has a direct business relationship with its customers (Sherman). Neither law requires "data brokers" to report on the type or use of data in their possession. Both state laws also neglect to establish the authority to monitor commerce by such entities. Consumers are left without protection or a clear path of redress, while companies can skirt the law to abuse the most private data available.

Nowhere are the impacts of such legislative negligence more evident than the exploitation of mental health data by data brokers post-COVID lockdown. In a study published

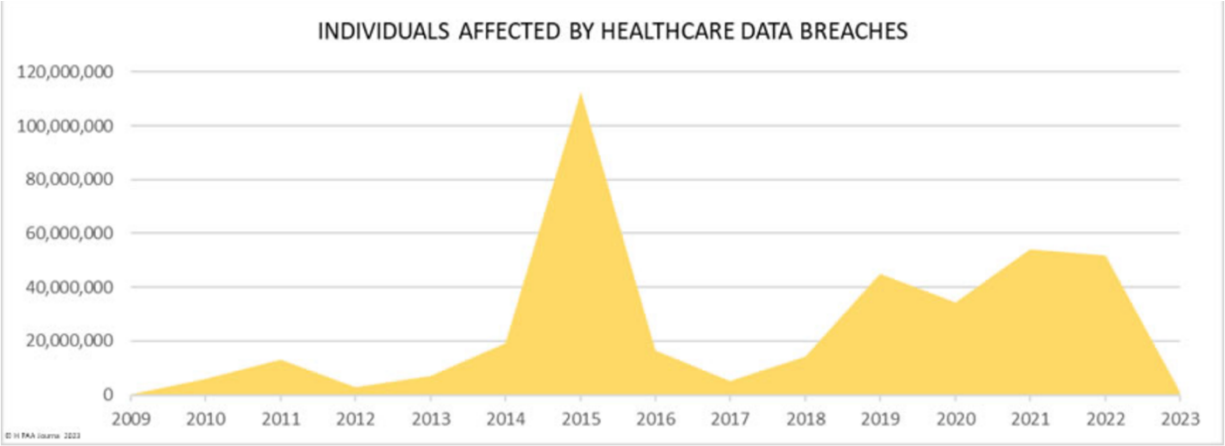
in February 2023, a research team at Duke University Sanford School of Public Policy found that data brokers are "marketing highly sensitive data on individuals' mental health conditions on the open market, with seemingly minimal vetting of customers and seemingly few controls on the use of purchased data" (Kim). Sensitive data was collected on telehealth and software application alternatives to in-person therapy sessions (mHealth). The study goes on to say that the data could be sold without deidentifying or aggregation. In other words, personal data on the specifics of one's psychological health could be bought and traced back to the individual without the patient ever knowing their information was sold.

This is what the Federal Trade Commission (FTC) alleges happened to the over 7 million consumers of the mobile health service Better Help. While promising to keep patient information confidential, the company used patient email addresses to market unique therapy options to all current and former clients on Facebook (Nguyen). The FTC was able to fine the mobile health service for violating its privacy promises after a complaint was filed by consumers but, the complaint did not promise any action will be taken to retrieve their personal information. Many of the FTC complaints filed are not remedied, or the solutions they do receive do not take actionable steps in reclaiming their personal information. The solution to the epidemic of unchecked data brokers who are selling individual identifiable health information is to provide a baseline of health privacy protection that guarantees a consumer's privacy and security, as HIPAA does. The federal law "limits the use or disclosure of PHI (personal health information) for marketing" (DHHS), effectively putting an end to the sale of medical data to data brokers.

Cost Analysis

From 2009 to 2022, the Department of Health and Human Services' Office for Civil Rights, known as the OCR, received reports of 5,150 healthcare data breaches that involved 500

or more records (HIPAA Journal). These breaches led to the exposure or unauthorized disclosure of 382,262,109 healthcare records, which is more than the population of the United States (HIPAA Journal). In 2018, healthcare data breaches of 500 or more records were being reported at a rate of approximately one per day (HIPAA Journal). Five years later, the rate has more than doubled. In 2022, there were an average of 1.94 healthcare data breaches of 500 or more records reported per day (HIPAA Journal). Below is a graph that demonstrates the scope of these data breaches from the point of view of the individual.

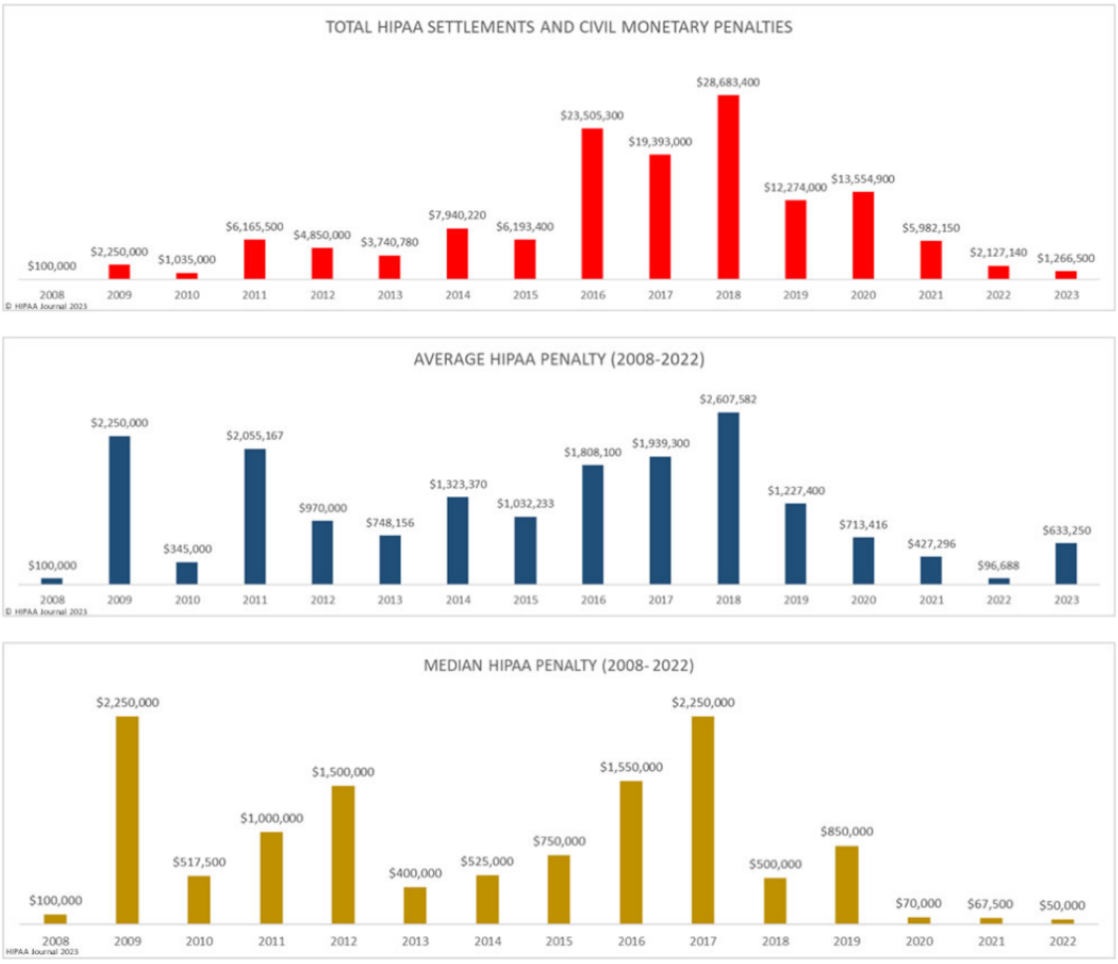


(Fg. 1 “Individuals Affected by Healthcare Data Breaches”. HIPAA Journal)

The trend for the number of exposed healthcare records has generally been upward over the years, with a significant spike in 2015, as represented in the graph. This year stands out as the worst in history for healthcare record breaches, with more than 112 million records exposed or disclosed without permission. Three major data breaches at health plans - Anthem Inc, Premera Blue Cross, and Excellus - contributed significantly to this trend in 2015 (HIPAA Journal). The breach at Anthem affected 78.8 million members, while the Premera Blue Cross and Excellus data breaches impacted around 10 million or more individuals each (HIPAA Journal).

Not only are the millions of health data breaches happening, but each one costs HIPAA covered entities an incredibly large amount. For example, Anthem Inc paid the largest financial

penalty for HIPAA violations ever recorded in 2018, settling for $16 million due to potential violations of the HIPAA Security Rule that came to light during the investigation of its 78.8 million record data breach in 2015 (HIPAA Journal). Premera Blue Cross settled for $6,850,000 in 2020, while Excellus Health Plan reached a $5,000,000 settlement in 2021, both resolving potential HIPAA violations linked to their respective 2015 data breaches that exposed the PHI of almost 10.5 million and 9.4 million individuals (HIPAA Journal). Significant financial penalties continue to be imposed on bigger companies, and smaller healthcare organizations are also no longer able to escape HIPAA fines, with 55% of financial penalties imposed by OCR in 2022 being on small medical practices (HIPAA Journal). The distribution of penalties since 2008 are shown in figure two below. Each one is slightly different than the previous, starting with the total monetary value of settlements per year, followed by the average HIPAA penalty, and lastly the median penalty value. Although different, each graph depicts the startling cost posed by data breaches and highlights a point that will be discussed further; the majority of penalties and data breach incidents occurred after 2013.



(Fg. 2 HIPAA Data Breach Penalties. HIPAA Journal)

Overall, HIPAA violations are not taken lightly. This strict enforcement provides a strong foundation for medical data security, with harsh fines used to punish entities that don't comply. This tough enforcement is used to make the privacy of identifiable health information a top priority. It has already been established that the cost of HIPAA compliance annually is estimated at $8.3 billion per year, however the proposed amendment to HIPAA is predicted to aid in the cost of compliance by reducing confusion on which entities are covered by the law and which are not. Ultimately, the costs of securing private medical data are high, but it is a necessity to ensure that the protection of this important information is a top priority.

Solution

We plan to expand what is considered a covered entity under HIPAA to be any entity that that buys and/or sells personal identifiable health data, namely data brokers. We also plan to add the stipulation that any data collected by parties via the internet of medical things, which is defined as "the network of Internet-connected medical devices, hardware infrastructure, and software applications used to connect healthcare information technology" will also be protected by HIPAA (Ordr). These devices include technology such as wearable fitness trackers, genetic testing sites, and mobile health apps. The original wording from HIPAA pertinent to this amendment is as follows:

> Covered entity means:
>
> (1) A health plan.
>
> (2) A health care clearinghouse.
>
> (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter, or
>
> (4) A business associate...

The amendment expands and makes considerations for the internet of medical things within the current understanding of health care clearinghouses. The National Institute of Health expands health care clearinghouses to mean:

> A public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value added" networks and switches that either process or facilitate the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction, or receive

> a standard transaction from another entity and process or facilitate the processing of health information into a nonstandard format or nonstandard data content for the receiving entity.

This understanding is ripe for development because the actions of clearinghouses today are almost synonymous with those of modern data brokerages. Updating "nonstandard data" to include data collected from "devices or sensors… that connect, communicate, or transmit information with or between each other through the Internet" includes the wide swath of patient health information available on the internet (FTC).

Strengths

By including this additional requirement, entities who collect data via the internet of medical things as a way to skirt around privacy regulation would no longer be able to exploit consumer privacy. Once HIPAA is expanded to cover all data brokers and those who collect personal health data through the internet of medical things, the risk of security threats on currently non-covered entities will diminish drastically. Because HIPAA limits the use and disclosure of personal health information, data breaches and stolen information are much less likely to occur. This is enforced through mandated encryptions, safeguards, and protections that ensure the security of identifiable health information. In addition, conflicts of data ownership and access will cease to exist. HIPAA makes it extremely clear who the personal data belongs to, which is the consumer. Furthermore, individuals are easily able to access, revise, or delete their private information from entities that possess it. Finally, an amendment to HIPAA solves the issue of unprotected identifiable data reaching the hands of data brokers. Since HIPAA limits the use and disclosure of personal health information to marketers, the personal health data of individuals will no longer be exploited for profit.

Elected officials such as Sen. Ron Wyden (D-OR), Sen. Patty Murray (D-WA) and Sen. Amy Klobuchar (D-MN) would be the biggest allies of HIPAA's expansion in this manner. Governmental entities such as the Department of Health and Human Services and the Federal Trade Commission would also agree with the solution we have proposed. The two bureaus advocate that this is a necessary amendment to protect health data privacy. Our proposal would prevent the selling of health data, protecting privacy, while still allowing an opportunity for general data broking, satiating industry's need for profit.

Weaknesses

As already noted earlier in this paper, HIPAA violations and their consequent fines have cost HIPAA covered entities millions annually. In fact, HHS estimates that the cost of HIPAA compliance is about $8.3 billion per year (Medical Economics). This issue, in the eyes of companies, would only be exaggerated by expanding HIPAA in the ways described above and could impede business through its prevention of the sale of identifiable health data. However, it would not entirely interrupt commerce. This proposal will not regulate the sale of de-identified health data, since it does not pose a security threat to individuals' privacy like identifiable health data. Furthermore, "HIPAA does not apply to health information about an individual that has been de-identified; however, entities covered by HIPAA must de-identify data in accordance with the HIPAA Privacy Rule" (DHHS). This would still allow entities to collect and use data for various beneficial reasons, but it would prevent private, identifiable, health data from being sold and circulated outside of the party that collects it. Additionally, strengthening HIPAA in this way would make it easier for businesses to navigate the privacy realm and avoid costly data breaches and their corresponding lawsuits. This fact can be attributed to that fact that they would

only have to look at one overarching piece of legislation to follow, rather than a confusing handful of smaller regulations based on location (HHS).

Opportunities

If HIPAA's definition of a covered entity were changed to include anybody who buys and sells personal identifiable health data as well as any entity that sells this information after collecting it through the medical internet of things, there could be several opportunities that arise.

One could be that with a broader definition of covered entities, there would be increased accountability and transparency in the healthcare industry. Any entity that handles personal identifiable health data would be subject to HIPAA regulations, and the penalties for violating them would be more severe. This could lead to a more secure and trustworthy healthcare system.

Companies that collect and sell health data could potentially develop new business models that align with HIPAA regulations. For example, a company that collects health data from wearables could become a covered entity under HIPAA and sell the data to healthcare providers for research purposes. This could create new revenue streams for these companies while also contributing to medical advancements.

By requiring more entities to adhere to HIPAA regulations, there would be a standardization of data sharing practices across the healthcare industry. This could improve collaboration between different healthcare providers and researchers, leading to more accurate diagnoses and better patient outcomes.

Patients would have greater control over their health data and how it is shared. The broader definition of covered entities could lead to stronger privacy and security protections for patients, which would be particularly important as more health data is collected and shared through the medical internet of things.

With a more secure and transparent healthcare system, there could be greater incentives for innovation in the healthcare industry. This could lead to new technologies and treatments that improve patient outcomes and overall health.

Threats

The most prominent threat to these amendments to HIPAA would be stakeholders such as companies that profit off the buying and selling of health data, their affiliates and shareholders, as well as individuals who are generally against governmental intervention of business. The expansion of HIPAA could adversely affect profit-making mechanisms for companies, resulting in the reallocation of resources, such as laying off employees or increasing the prices of goods. Our proposed amendment would not completely eradicate the selling of data but limit it to identifiable health data. This would still allow for data brokers and companies to turn a profit while simultaneously protecting the general public's private health data.

Conclusion

While HIPAA has been a crucial piece of legislation in protecting individuals' health information, it has not kept up with the rapid technological advancements that have occurred since its inception in 1996. With the rise of new stakeholders in the healthcare industry, including data brokers, HIPAA's boundaries have been surpassed, leaving individuals vulnerable to having their health data collected and sold without their consent. Data brokers present a unique threat to personal health data, and current state laws lack the necessary oversight and regulation to monitor commerce by such entities. It is necessary to approach this problem from the federal level and expand HIPAA's definition of a covered entity to ensure that individuals' health data remains protected from exploitation by data brokers and other stakeholders in the healthcare industry.

Sources

Bello, Ryan S. and Dena, Castricone M.. "Overview of 2013 Amendments to HIPAA Privacy, Security, Breach Notification and Enforcement Rules." Duane Morris LLP, 22 April 2013, https://www.duanemorris.com/alerts/overview_2013_amendments_to_HIPAA_privacy_security_breach_notification_enforcement_rules_4734.html.

California Office of the Attorney General. "California Consumer Privacy Act (CCPA)." California Office of the Attorney General, https://oag.ca.gov/privacy/ccpa. Accessed 8 Apr. 2023.

Centers for Disease Control and Prevention. “Health Insurance Portability and Accountability Act of 1996 (HIPAA).” Centers for Disease Control and Prevention, Centers for Disease Control and Prevention, 27 June 2022, https://www.cdc.gov/phlp/publications/topic/hipaa.html.

Downey, Aubrey. "HIPAA: What Cost?" Medical Economics, 20 Aug. 2015, https://www.medicaleconomics.com/view/hipaa-what-cost.

Federal Trade Commission. “Internet of Things: Privacy & Security in a Connected World.” Federal Trade Commission, 27 Jan. 2015, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

Grand View Research. "Electronic Health Records (EHR) Market Size, Share & Trends Analysis Report By Product (Web/Cloud-based, On-premise), By Component, By End Use (Hospitals, Clinics), By Region, And Segment Forecasts, 2021 - 2028." Grand View Research, 2021, https://www.grandviewresearch.com/industry-analysis/electronic-health-records-ehr-market.

HIPAA Journal. "Healthcare Data Breach Statistics." HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/. Accessed 8 Apr. 2023.

Hoey, Peter, et al. “Healthcare's Data Tsunami.” Brunswick Group, 23 February 2022, https://www.brunswickgroup.com/healthcare-data-i20729/. Accessed 8 March 2023.

Husch Blackwell. “Colorado Privacy Act Resource Center: Husch Blackwell.” Husch Blackwell | Husch Blackwell, 2022, https://www.huschblackwell.com/industries_services/colorado-privacy-act.

Kim, Joanne. “Data Brokers and the Sale of Americans' Mental Health Data.” Tech Policy @ Sanford, https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/02/Kim-.

Klein, Ron. "Digital Health's Role in Managing Chronic Disease." Forbes, 29 Oct. 2021, https://www.forbes.com/sites/forbestechcouncil/2021/10/29/digital-healths-role-in-managing-chronic-disease/?sh=734815b7735c.

Nguyen, Stephanie T., et al. “FTC says online counseling service BetterHelp pushed people into handing over health information – and broke its privacy promises.” *Federal Trade Commission*, 3 March 2023, https://www.ftc.gov/business-guidance/blog/2023/03/ftc- says-online-counseling-service-betterhelp-pushed-people-handing-over-health- information-broke. Accessed 8 March 2023.

Peters I. HIPAA-Covered Entities: It's Time to Cover Yourself. The National Law Review.; 2018. Available from: https://www.natlawreview.com/article/hipaa-covered-entities-it-s-time-to-cover-yourself

U.S. Department of Health and Human Services. "Non-Covered Entities Report." HealthIT.gov, 17 June 2016, https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf.

"What is IoMT? - Ordr." Ordr, n.d., https://ordr.net/article/what-is-iomt/.