Virtually Defenseless in a Digital Era:
The Necessary Revisions HIPAA Must Adopt in the Twenty-First Century

by

Min K. Song

Bachelor of Arts, University of Pittsburgh, 2020

Juris Doctor, University of Pittsburgh School of Law, 2024

Submitted to the Graduate Faculty of the

School of Public Health in partial fulfillment

of the requirements for the degree of

Master of Public Health

University of Pittsburgh

2024

UNIVERSITY OF PITTSBURGH

SCHOOL OF PUBLIC HEALTH

This essay is submitted

by

Min K. Song

on

April 16, 2024

and approved by

Evan S. Cole, PhD, MPH, Research Associate Professor, Health Policy and Management,
University of Pittsburgh School of Public Health

Reena S. Cecchini, PhD, MS, Research Assistant Professor, Biostatistics,
University of Pittsburgh School of Public Health

Virtually Defenseless in a Digital Era:
The Necessary Revisions HIPAA Must Adopt in the Twenty-First Century

Min K. Song, MPH

University of Pittsburgh, 2024

In the wake of rapid technological advancements, the convergence of location data and artificial intelligence poses significant challenges to an individual's right to health privacy in the United States. This paper explores the implications of this intersection, particularly regarding the use of inferred protected health information (PHI) outside the purview of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Despite the earnest attempt to safeguard PHI, the statute is useless when put against modern digital advancements. Through a thorough examination of current regulatory gaps and recent events, the paper underscores the critical need to move forward with necessary revisions to current HIPAA provisions. Failing to address these concerns will undermine an individual's fundamental right to privacy and ultimately lead to distrust in the healthcare institution. The urgency to address these evolving threats will persist until concrete action is taken to hold non-regulated entities accountable and establish measures to guarantee the protection of future generations' PHI from malicious actors.

Table of Contents

Preface

Dedicated to the woman who taught me to always have my heart in my work and never quit.

Thank you, mom. You inspire me every day.

1.0 Introduction

An individual’s locality has been tracked for decades. Until the 20th century, location data only measured stationary information: addresses of workplace or residence. Nonetheless, the Supreme Court of the United States held that an individual has a constitutional right to the expectation of privacy, which may be violated by a physical or electronic intrusion.

With the epochal shift into the digital era, tracking has now bled into mobile movement, leading to an expansive collection of location data. The information is akin to a gold mine when coupled with artificial intelligence. By applying this technology to location data, private and public entities can infer an individual’s next move, purchase, and startlingly, health conditions. Significant health policy concerns rise with these advancements; entities not subject to the regulations of the Health Insurance Portability and Accountability Act of 1996 may gather health data and exploit the information for nefarious ends. This would result in endless court claims filed by individuals seeking redress for the breach of their health privacy rights, and a loss of trust in the healthcare system. Today, there is virtually no reporting on this matter. Nonetheless, the absence of widespread media coverage does not justify the failure to establish protection measures before the situation escalates. Implementing preventative measures today will alleviate the inevitable future strains on the healthcare system.

This paper will explore how location data and artificial intelligence intertwine in the digital era, and why a revision to HIPAA is not only necessary, but urgent.

2.0 The Only Health Privacy Statute

2.1 Pre-HIPAA Era

Medical records document intimate details concerning various aspects of an individual’s life, ranging from physical health to interpersonal relationships. Prior to 1996, there was no federal protection for these records. Thus, the distribution of medical records did not require patient consent. It was common practice to penalize individuals based on their medical records. Employers factored in health to determine promotions, insurance companies set higher premiums for chronically ill consumers, and landlords refused tenancy to physically disabled applicants.

2.2 Enactment of HIPAA

At the tail end of the twentieth century, Congress passed what would be the first and last of its kind, the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA was enacted with these guiding principles: prioritizing individuals' privacy rights, fostering trust between patients and healthcare providers, and mitigating stigma associated with health conditions. Ultimately, the act was passed to ensure compliance amongst healthcare providers and prevent the unauthorized disclosure of health information.

2.2.1 Key Definitions in HIPAA: Covered Entities, Business Associates, PHI

Amongst many, these key terms were defined: covered entities, business associates, and protected health information (PHI).

Covered Entities: A health plan, a health care clearinghouse, [and] a health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter (45 CFR § 160.103; 45 CFR § 164.104).

Business Associates: A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information, a person that offers a personal health record to one or more individuals on behalf of a covered entity, [and] a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate (45 CFR § 160.103; 45 CFR § 164.104).

Protected Health Information (PHI): Individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral, excluding certain educational and employment records (45 CFR § 160.103).

2.2.2 Delegation of Regulatory Authority to HHS

HIPAA, in large, was passed to limit covered entities and business associates' handling of PHI. The U.S. Department of Health and Human Services (HHS) was delegated the authority to create regulations that would enforce HIPAA. In response, the HHS promulgated the following HIPAA regulations that must be followed by covered entities and their business associates:

Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) and Security Standards for the Protection of Electronic Protected Health Information (Security Rule).

2.2.3 HIPAA Regulations: Privacy Rule and Security Rule

The Privacy Rule is a series of requirements for the use and disclosure of PHI. Its purposes are to safeguard PHI, while allowing the necessary flow of information for healthcare services (Health Insurance Portability and Accountability Act [HIPAA] of 1996, Pub. L. No. 104-191). Under the rule, covered entities and their business associates may share PHI only with the individual, and the usage of PHI must only be for treatment and payment (with enumerated exceptions). A key component to the Privacy Rule is the Minimum Necessary Standard. Outlined in 45 CFR § 164.502(b), this standard requires covered entities to use the minimum amount of PHI necessary to achieve its intended purpose. This applies for both internal and external disclosures. The impact on covered entities created by the Privacy Rule may be found in their policies, such as access control (e.g., limiting access to PHI based on job responsibilities).

The Security Rule orders covered entities to "maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting [electronic protected health information] e-PHI." More specifically, their duties under the rule are to "[e]nsure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit; [i]dentify and protect against reasonably anticipated threats to the security or integrity of the information; [p]rotect against reasonably anticipated, impermissible uses or disclosures; and [e]nsure compliance by their workforce" (Health Insurance Portability and Accountability Act [HIPAA] of 1996, Pub. L. No. 104-191). To ensure compliance, covered entities often encrypt ePHI to protect it from unauthorized access and interception.

3.0 Location Tracking in the Digital Age

Two decades into the twenty-first century, smartphones revolutionized technology’s role in everyday lives due to their internet connectivity, multimedia capabilities, and app ecosystems. Pew Research Center reported that 97% of Americans own a smartphone ("Pew Research Center," n.d.). These devices accompany individuals *everywhere* – restaurants, your mom’s house, concerts, and bathrooms. This is a known fact and can be proven through Global Positioning System (GPS) points. GPS technology leverages satellite signals to determine the location of any smartphone, and consequently, the individual. Location data is the digital trace created by the movements of the smartphone. While the physical location is derived from IP addresses associated with landlines, GPS signals from mobile devices are used to gather the location data. It is commonplace for smartphone apps to frequently access and gather location data.

3.1 Mobile Devices and Location Data

The vast collection of location data that takes place today would be unfathomable to the legislators who drafted HIPAA two decades ago. In a 2019 New York Times opinion article, journalists presented a series of satellite images depicting hundreds of green dots, each representing an individual’s smartphone location (Kolata, 2012). The images depicting location data were generated by analyzing a vast dataset containing real-time location points from over 12 million smartphones across several major cities. The precise location of each smartphone was traceable down to the minute from the years of 2016 - 2017. To illustrate the ease of linking a single ping to an individual, the journalists presented an image of Central Park with a lone green dot. The subsequent image zoomed out to display the entirety of Manhattan, now populated with hundreds of green dots, indicating every location visited by that one smartphone during a specified period. Finally, the images connected each green dot, forming a precise map of the individual's movements throughout the year.

Studies have proven most individuals are unaware of their location data being collected by companies, let alone what they consent to such information being used for. An empirical study conducted by professors Kirsten Martin and Helen Nissenbaum explored individuals' knowledge about location data and its relation to their expectation of privacy (Nissenbaum, n.d.). The professors used a factorial vignette survey and surveyed 1,500 study participants across the country. Study participants were asked to rate the appropriateness of how location data was being collected. Elements of the survey were location, actor, source, place, duration, and time. The results from the study indicated that individuals felt their privacy was violated when companies tracked their location in public and private settings. The study revealed that the notion of "public is public" was not right, and that there is a "strong, nuanced, and systematic privacy expectation in spaces and places typically considered public" (Nissenbaum, n.d.). The rift of how individuals understand location data surveillance to work, and how companies conduct such surveillance, creates a great misunderstanding of consent given to those companies.

3.2 Location Data and Artificial Intelligence

Artificial Intelligence (AI) is a broad field that encompasses both technology and software to synthesize, perceive, or infer information that ordinarily involves human intelligence. By leveraging the advance mechanics of a computer to achieve correct inferences, AI’s capabilities vary vastly in difficulty, ranging from predicting text messages to curating the perfect TikTok algorithm. This refers to predictive AI algorithms, which utilize historical data and machine learning technology. The predictive AI algorithm analyzes the information, seeks out trends, and then makes its predictions based on the available information. Such inferences may seem innocuous, even beneficial. From 2020 to 2022, Google used AI and aggregated location data to monitor individuals’ movements in response to the global pandemic (Google. n.d.). The company’s goal was to “remediate the impact of COVID-19” by publishing its findings, and have the information used by individuals and policymakers alike for informed decision-making (Google LLC. n.d.). The American Red Cross has employed AI and location data for “Safe & Well" (American Red Cross, 2011). This app utilizes location data and AI to provide necessary resources for its users amidst natural disasters. However, when the algorithm infers health conditions from location data it takes a sinister turn.

3.3 Location Data and Artificial Intelligence: As Used by Third Parties

3.3.1 General Purposes

Unbeknownst to many, third party companies partner with choice mobile app providers to receive location data information. One such company being Cuebiq, who's business area is location intelligence and spatial analytics (Cuebiq. n.d.). They offer clients "offline location analytics, real-time audience optimization [and] geo-behavioral audiences for cross-platform ad targeting" (Cuebiq. n.d.). It should be noted that in addition to mobile devices, location data is collected by technology that does not require internet connectivity (i.e., closed network infrastructures, mobile device sensors).

Offline location analytics is the aggregated collection of historic location data relating to individuals' movements in physical spaces. Data harvesters examine patterns and trends to better understand consumer tendencies and provide insight to its clients. Per instance, Walmart uses this analysis to understand how traffic patterns impact its consumers' behaviors.

Real-time audience optimization is the practice of using location data and AI to continuously monitor real-time location and behavior. This data includes individuals' engagement with online activities, digital platforms, and marketing campaigns. The data is collected in real-time, allowing organizations to respond immediately with personalized interactions based on the individual's current behaviors and preferences. Per instance, Amazon continuously analyzes their customers' interactions with the website (Amazon Web Services, n.d.). Using this ongoing analysis, it will and adjust its product recommendations accordingly.

Geo-behavioral audiences are specific segments of consumers categorized by their location-based behaviors and activities. These "audiences" are created by applying AI to location data that then identify patterns and trends that uniquely fit their group. Overall, this categorization enables marketers to target distinct audiences more effectively.

Clients find products like offline location analytics, real-time audience optimization and geo-behavioral audiences invaluable. Insight into a group's behavior, visitation patterns, and demographic characteristics are indispensable in today's business environment. Even detailed information about a single person's is valuable to companies today. A file of an individual's preferences enables companies to have a completive edge to develop customized services.

3.3.2 PHI Purposes

As forementioned, when applied to location data, AI is capable of correctly inferring various aspects of an individuals' life. Looking at the products offered by Cuebiq through a public health lens, there is a clear gap in privacy protection for non-covered entities that HIPAA has yet to fill. This section will explore health-related location data in the lens of the three products offered by companies like Cuebiq.

Using offline location analytics, such as movement patterns, AI can derive insights into an individual's health conditions. Movement patterns may demonstrate sudden decrease in mobility and frequent visits to a hospital. This information may be used by retail companies to infer the individual is experiencing health concerns and use data to further determine specifics. Per instance, businesses may send targeted ads for health products to an individual. This action blurs the lines between consumer data analytics and healthcare privacy, raising ethical questions about the use of personal information for commercial purposes.

Real-time audience optimization techniques for inferring health conditions often involve two key components: identification of key locations and behavioral analysis. With real-time processing algorithm, third parties may identify key locations visited by individuals and the frequency and duration of those visits. Using this information, AI can infer an individual's behavioral patterns. Regular attendance at a gym suggests an active lifestyle, whereas spending limited time at home during typical sleep hours implies irregular sleep patterns, potentially linked to disorders or stress.

Third parties leverage geo-behavioral audiences to encourage certain acts or plan interventions. Pharmaceutical firms use insight from geo-behavioral audiences to create targeted health campaigns. This may involve online platforms targeting specific demographics due to their group's unique health conditions. Nonprofit organizations may use this information to investigate how access to green space influences a geographic group's physical activity levels and overall health.

All this information begs the question: who has the capability to buy location data, and what channels are used to obtain it? The answer to these questions is relatively straightforward. Location data is often purchased by tech companies, research firms, government agencies, and financial institutions. To obtain location data, these entities may choose between direct purchase or collaboration with the data collector in some form. The ease of acquiring location data depends on several factors, including the intended purpose of the data, existing regulatory requirements, geographic location, and the nature of the data sought.

It's worth noting that businesses frequently supply their employees with cell smartphones. As company property, employers have the legal right to enable monitoring software onto these devices to review its employees' actions (ADP, n.d.). Since COVID-19, the number of employers who use such software has doubled, due to its ability to show employees' "productivity trends by tracking the time spent on tasks. [It] can determine which team members are fully engaged and which are wasting time on unproductive apps and websites” (CurrentWare, n.d.). Despite not directly purchasing location data, it's crucial to recognize that businesses still have access to their employees' location data.

The information inferred by AI using location data, as described above, is safeguarded under HIPAA as PHI. However, since none of the third parties are classified as covered entities or business associates, they are not subject to regulation under this statute. As a result, non-covered entities may infer an individual's health conditions without statutory limitations on how the information is utilized or distributed.

The accurate inference of health conditions by non-covered entities undermines individuals' rights to PHI, bypassing consent mechanisms and accountability standards outlined by HIPAA. This intrusion leaves individuals vulnerable and exposed, especially if the inferred information is sensitive or stigmatizing, such as mental health conditions or chronic illnesses. As a result, this could lead to a decrease in trust in healthcare systems, perpetuating a cycle of consequences. The diminished confidence may strain patient-provider relationships and contribute to adverse health outcomes. The resulting reputational damage to the institution could have significant and widespread societal implications. Furthermore, under the current legal landscape, individuals lack the ability to pursue legal action against non-covered entities for violations of protected health information (PHI) under HIPAA. In a cyclical manner, this heightens the likelihood of privacy breaches and exacerbates the erosion of trust in the healthcare system.

4.0 Public Health Relevance

The intersection of location data, AI, and the ability of organizations to infer personal health information outside the purview of HIPAA regulations poses significant public health concerns. public health and maintaining trust in healthcare systems. These entities, ranging from corporations to government bodies, possess significant authority to utilize inferred PHI for various purposes without adhering to the usual constraints that hold covered entities and business associates under HIPAA accountable.

Distinguishing between mere data points and drawing inferences from it is crucial. Without drawing conclusions from location data points, they remain mundane details and lack significant value. For instance, consider a man who routinely walks to the corner of 68th street and 3rd avenue every weekday at 9 AM. Detected and cataloged as a data point in his personal location file, it is at this point useless. However, when AI systems are employed to identifying the location's attributes, the value of this information skyrockets. If, for example, a cycling studio is located at that corner, AI systems may infer the man is engaging in exercise. Private entities could exploit this information by sending him targeted advertisements for workout gear and continue to categorize him accordingly for future marketing campaigns. Conversely, if the location was replaced with a methadone clinic, AI systems may infer the man is seeking medical treatment for substance use disorder. This could result in the man being profiled with a health issue. Such profiling by third parties and its potential consequences directly contradicts the intent of HIPAA. Substance use disorder treatment falls under PHI for medical history. However, the nature of inferences and profiling in this scenario may not be protected under HIPAA for several reasons. Firstly, non-health related entities often do not fall under HIPAA's jurisdiction. Additionally, the information was collected by AI systems inferring conditions from location data, whereas HIPAA primarily safeguards existing PHI usage and disclosure. Consequently, the current legality of making such inferences from location data to determine an individual's health condition remains uncertain.

Media coverage of a methadone clinic targeting campaign may be limited, but the issue is far from unrealistic. Back in 2017, Copley Advertising, LLC, was hired to direct targeted advertisements to "abortion-minded women" in waiting rooms at health clinics using geofencing in Massachusetts (Massachusetts Attorney General, n.d.). Geofencing works by creating a virtual "fence" around a specified location, triggering when a person crosses it with a mobile device. Once triggered, advertisers tailor ads to the individual’s device. In this case, ads included "Pregnancy Help" and "You're Not Alone" messages, directing users to abortion alternatives websites and access to live chats (Massachusetts Attorney General, n.d.). Massachusetts brought legal action against Copley, alleging it violated privacy laws by tracking consumers' physical locations near medical facilities, disclosing information to third-parties, and tailoring medical ads to patients without consent. The circumvention of HIPAA consent mechanisms undermines the protection of PHI and will inevitably deter individuals from seeking essential medical care.

The erosion of trust will ultimately lead to negative health consequences, as individuals may fear being identified in certain healthcare settings or hesitate to disclose important health information. Addressing the regulatory gaps surrounding the utilization of location data for health inference is paramount for both safeguarding public health and upholding trust in the healthcare institution.

5.0 Gap Analysis

Under the HIPAA Privacy Rule, the definition of covered entities is limited to healthcare providers, health plans, and healthcare clearinghouses. Historically the concise list was sufficient as these three groups were the primary custodians of PHI. However, due to rapid technological advancements, this is no longer the case. Today, non-healthcare entities have access to information that would otherwise be PHI if it were disclosed to a covered entity. These non-healthcare entities have access to such information by using things like location data and AI to infer health conditions.

Health-adjacent devices are extremely popular amongst the public today due to its vast range of coverage. Health apps, fitness trackers, and remote monitoring tools can now capture information like menstrual cycles, heart rate readings, and dietary intake. In 2023, there were 311 million health app users, and the fitness trackers market saw notable expansion due to consumers favoring wearable technology (Business of Apps. n.d.). These technologically driven devices transmit the collected data back to the respective company for analysis and storage. This implies that third parties are storing the health information of millions of individuals. Currently, HIPAA regulations do not apply to these health-adjacent devices as they neither qualify as covered entities nor are integrated with one. Consequently, the sale of the information to non-healthcare entities is not regulated, leading to a series of dilemmas. If the purchaser of the data is a third-party company that has access to individual’s location details, they can then utilize AI to deduce PHI from the obtained data.

The widespread use of health-adjacent devices has led to the collection and transmission of sensitive health information without being subject to HIPAA regulations, raising significant privacy and security concerns. There is a need to establish a regulatory framework specifically tailored to health-adjacent devices to ensure adherence to stringent privacy and security standards. The framework should encompass data collection, storage, transmission, and access protocols. Additionally, consideration should be given to expanding HIPAA regulations to include health-adjacent devices and the entities involved in their operation. Public awareness and education efforts are crucial to empower individuals to make informed decisions about the use of such devices and advocate for their privacy rights. Moreover, collaboration among stakeholders, including technology companies, healthcare providers, advocacy groups, and legislators is essential. Actions that result in regulatory solutions to protect individuals' privacy in the digital healthcare era is crucial to ensure PHI safeguard.

6.0 Stakeholder Analysis

A growing list of advocacy groups have championed individuals' rights to privacy and civil liberties regarding AI inferred data. Among these organizations, the Electronic Frontier Foundation (EFF) and Patient Privacy Rights (PPR) have been instrumental in advocating for concerns surrounding location data and the AI-based deduction of health information.

6.1 Non-Profit Entities

6.1.1 Electronic Frontier Foundation (EFF)

In the 2017 Supreme Court case Carpenter v. United States, the EFF filed an amicus brief vehemently objecting to the warrantless gathering of location data (Electronic Frontier Foundation. n.d.). The organization emphasized two primary concerns. Firstly, that such data may unveil detailed aspects of individuals' personal lives. Secondly, the increased concerns regarding third party's ability to retrospectively reconstruct past movements, further encroaching into individual's private life. While not directly addressed in the brief, the privacy concerns raised could carry substantial implications for health information. Location data may reveal an individual's healthcare facility visits, undermining the confidentiality safeguarded under HIPAA's Privacy Rule. EFF released the opinion piece, *Don't Mix Policing with COVID-19 Contact Tracing*, during a critical phase of the pandemic (Electronic Frontier Foundation, 2020). At that point, contact tracing was vital for containing the virus and resulted in individuals continuously sharing their location with third parties. The EFF expressed concern that individuals may hesitate to engage in contact tracing efforts if they feared their location data could be accessed by law enforcement. The text raised concerns regarding risks of personal information being accessed by law enforcement for purposes unrelated to public health (e.g., interrogating protesters, conducting social media surveillance on dissident movements). The piece argued such practices infringe upon several Constitutional rights. The significance of data minimization and establishing a clear demarcation between public health initiatives and law enforcement actions was consistently underscored. The conclusion emphasized the critical role of these measures in preserving public trust in the healthcare system and at times where location surveillance is vital (i.e., during a pandemic).

6.1.2 Patient Privacy Rights (PPR)

PPR was crucial in advocating for additional privacy and security protections in the Health Information Technology for Economic and Clinical Health Act (HITECH) (U.S. Department of Health & Human Services. n.d.). Due to the growing digital healthcare environment, PRR recognized the necessity of enhanced patient information safeguards within federal statutes. The organization engaged in lobbying efforts and collaboration with lawmakers to such protection from unauthorized access and misuse. Since 2012, PRR has actively supported the DataMap project, an initiative to track and document the flow of personal data (e.g., location data), within the healthcare sector (Patient Privacy Rights. n.d.). That same year, PRR introduced its Privacy Trust Framework, a comprehensive set of over 75 auditable criteria designed to evaluate how digital tools and platforms safeguard health information privacy (Patient Privacy Rights. n.d.). PRR's objective was to empower healthcare providers to make well-informed decisions for technology systems that offer optimal protection of PHI.

6.2 Private Entities

Advocacy groups continue to raise concerns about the threats posed to PHI by technological advancements and advocate for enhanced, federal patient privacy rights. Conversely, there are numerous entities opposed to such changes. Corporate entities collect vast amounts of data, including location and health-related information, for the purposes of targeted advertising and product development. These companies are often against heightened federal and state privacy laws. They show their disdain for such changes through lobbying efforts and contributions to partisan parties.

6.2.1 Google

Google dominates the search engine market and is synonymous with information retrieval. Such a prolific reputation is due to its highly tailored results for individuals by using their personal data. With location logs and health history, Google personalizes an individual’s recommendations for clinics and fitness facilities based on their highly specific characteristics and preferences. Google publicly emphasizes a commitment to privacy in its policy statement, but its actions suggest otherwise. Google's lobbying expenses often amounts to millions of dollars every fiscal quarter and are often involved in the realm of privacy laws (Statista. n.d.). In 2018, the first online privacy law was passed in California (California Attorney General. n.d.). The state law created the right to know, access, and request deletion of personal data held by tech companies. In alignment with the other tech giants, Google, expressed concern about the law's impact and sought last-minute changes to exempt certain data collection practices, even if users opted out. Nevertheless, state legislators ensured that individuals retained the ability to opt out.

6.2.2 Meta (Formerly Facebook)

Meta (formerly known as “Facebook) gathers users location data and health information to enhance the platform's functionality and personalize content and advertisements. The profitability attributed to its data collection practices is undeniable. By leveraging this data for more curated experiences, the website has experienced higher click-through rates and engagement. According to Federal Election Commission, back in 2021 top executives of Meta made a minimum of $3.9 million in political donations (Hernandez, 2019). The significant monetary contributions demonstrate Meta’s vested interest in shaping legislation directly involving the tech industry and privacy laws.

With less stringent privacy laws, corporate entities can assert greater control over data, enabling them to maintain a competitive edge in the market. Therefore, they are likely to find a revision to HIPAA less than favorable.

7.0 Remedies to Address Public Health Concerns

7.1 Federal Proposal: Broaden HIPAA

The problems regarding health privacy that arise today are partially because HIPAA is the only federal health privacy law. With the growing digital nature of society, the Privacy Rule and Security Rule no longer serve their purpose in safeguarding PHI. This section will explore two recommendations on how to revise HIPAA to meet modern needs and once again ensure health privacy.

7.1.1 The Privacy Rule - Redefining the Key Terminology

Given the evolvement of technology and continuous location monitoring, key definitions within the regulation should be revised to encompass these changes.

Covered entities should be revised to encompass any entity capable of employing AI to infer PHI. Suggested terms include “PHI-inferencing entity" and "AI-enabled PHI predictor." These terms are tailored specifically to encompass organizations capable of inferring PHI from location data. The definition is broadened to encompass non-healthcare entities (i.e., mobile and tech companies) whose ability to deduce health conditions warrants regulation under HIPAA. This would expand the Privacy Rule to tech conglomerates like Google, Apple, and Amazon. Expanding the protection beyond healthcare providers would result in enhanced protection of individuals' health information across multiple industries. This would ensure AI-utilizing entities adhere to the strict privacy standards of HIPAA, such as regulating how the PHI is used, stored, and shared. The beneficial effects would extend across various sectors, fostering heightened transparency and accountability in personal data management. The definition is adequately narrow to avoid the absurd outcome of encompassing too many irrelevant parties under the Privacy Rule. This ensures the prevention of wasted legal resources and backlash resulting from ambiguous regulation edits.

Similarly, the definition of business associates should extend to any entity that collects personal data for the purposes of health analysis or transmission. The change would expand the Privacy Rule to healthcare-adjacent devices that are not currently regulated under HIPAA such as mobile health apps, fitness trackers, and remote monitoring devices. This would regulate the sale of health information to non-healthcare entities. Extending the definition of business associates under HIPAA is essential to cover all potential sources of PHI exposure, given their varied functions. Narrowing the definition to include only AI-utilizing entities would enhance privacy regulation as AI becomes more widely used.

Additionally, PHI should cover health data inferred from AI when combined with other information to identify individual’s health status, condition, or treatment. The modification would ensure PHI regulations stay pertinent and effective in safeguarding individuals' privacy amid the growing influence of AI-driven health data analytics.

7.1.2 The Security Rule – Revamping Standards

A revision to the Security Rule is necessary to further protect PHI during such a technologically advanced age. One such measure can be to mandate enhanced data encryption measures. This would require covered entities to implement robust encryption techniques for all data, including location information, to mitigate the risk of unauthorized inference of PHI by AI algorithms. With such strengthened measures, even if AI algorithms analyze the encrypted data, the system would be unable to extract meaningful information without access to the decryption key. This may create a stronger barricade between PHI and third parties seeking access to the information.

Given its rapid proliferation, it is imperative to dedicate a provision within the Security Rule to geofencing. The lack of transparency of such technology being used violates privacy rights and leads to unauthorized disclosure or exploitation of the inferred PHI. In essence, the legality of utilizing this information hinges on obtaining informed consent and ensuring ethical data practice Presently, individuals are broadly unaware of location-data collection activities, and unethical use, particularly for health-related marketing purposes, persists under current regulations. For informed consent, the regulation should mandate covered entities employing geofencing technology to provide transparent notice and obtain explicit consent from individuals entering the designated area. To promote ethical practices, covered entities must establish appropriate safeguards for geofencing. This includes conducting thorough risk assessments and implementing encryption methods to safeguard patients' location data by anonymizing it. Effectively anonymizing the location data prevents targeted actions at individuals, while still enabling organizations to aggregate data (e.g., daily number of visitors to a clinic, without identifying specific individuals).

Moreover, the Security Rule should implement an auditing mechanism for entities regulated under HIPAA. This would come in the form of risk assessment and be utilized by these entities to determine hazards linked with technology. By mandating these assessments, a heightened standard for protecting PHI privacy will be further ensured.

7.1.3 The Implications of Broadening HIPAA

Expanding the scope of HIPAA may yield unintended consequences. Resistance to broadening the Privacy Rule may stem from concerns of negative outcomes for consumers, and more realistically the private organizations that profit from the information. Broader HIPAA regulations may decrease tailored search results, frustrating individuals accustomed to the convenience of personalized experiences. Expanding "covered entities" and "business associates" may subject HIPAA to unforeseen scrutiny in the court. Ultimately, private entities with deep pockets who are unpleased with the changes are likely to initiate unnecessary litigation claims, placing strain on the court system.

Revising HIPAA provisions presents formidable challenges. All changes must undergo official regulatory channels by the U.S. Department of Health and Human Services (HHS). The formal rulemaking process includes notice and comment periods, which are both time-consuming and resource-intensive. Policymakers and regulators consistently navigate the delicate balance between the need for regulatory updates and the imperative to uphold consistency, clarity, and effectiveness in their already promulgated rules. However, given the current and foreseeable issues, the need for revising HIPAA provisions is more than necessary.

7.2 State Proposal: Implement Privacy Acts

Another approach to safeguarding location data and the inference of PHI is for state legislators to adopt a statute similar to the California's Consumer Privacy Act (CCPA). CCPA provides various privacy protections to Californians, including rights to access, delete, and opt out of the "sale" of their personal data, which encompasses location data. State legislation follows a structured process, beginning with the introduction of a bill by legislators, followed by committee review, floor debate, and voting. If the bill passes both chambers, it is sent to the governor for approval. Enacting legislation similar to CCPA would effectively safeguard PHI from inference by location data and AI by ensuring individuals decide how their data is used.

8.0 Conclusion

Technology advancements have ushered in a new era where the intersection of location data and AI presents unprecedented challenges to health privacy. Despite the previously laid out safeguard by Congress, it is time to address HIPAA’s inadequacy in the digital age.

As highlighted throughout this paper, the lack of regulatory oversight for non-covered entities leaves individuals virtually defenseless to privacy threats. This brings great concern today as the judicial landscape continues to change rapidly. Today, thousands are concerned about changing reproductive health rights after the overturning of Roe v. Wade. A large part of the population is now critically vulnerable to privacy threats, especially in states where laws incentivize private citizens, often referred to as "bounty hunter laws,” to file civil complaints against individuals. There is an understandable fear that location data may track visits to sensitive locations such as Planned Parenthood clinics. Adversaries may exploit location data and AI to monitor individuals' movements and disclose visits to such facilities, leading to privacy violations and even harassment or discrimination.

Adapting legislation to mitigate evolving threats to PHI privacy would ensure the security of PHI and continue to nourish the trust between patients and healthcare system. Neglecting to do so would result in the loss of individuals' fundamental right to privacy and distrust in the healthcare system.

Bibliography

Rosenblat, A. (2012). Dredging Up the Past: Lifelogging, Memory, and Surveillance. University of Chicago Law Review, 75(1), Retrieved from https://chicagounbound.uchicago.edu/uclrev/vol75/iss1/3/

U.S. Department of Health & Human Services. (n.d.). HITECH Act enforcement interim final rule. Retrieved from https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html

Patient Privacy Rights. (n.d.). The DataMap. Retrieved from https://patientprivacyrights.org/thedatamap/

Patient Privacy Rights. (n.d.). Patient privacy rights. Retrieved from https://patientprivacyrights.org/patient-privacy-rights/

Electronic Frontier Foundation. (n.d.). Amicus brief in Carpenter v. United States. Retrieved from https://www.eff.org/document/amicus-brief-carpenter

Electronic Frontier Foundation. (2020, June). Don't Mix Policing with COVID-19 Contact Tracing. Retrieved from https://www.eff.org/deeplinks/2020/06/dont-mix-policing-covid-19-contact-tracing

The Cochrane Collaboration. (n.d.). Supports Free Access to All Data from All Clinical Trials. Retrieved from http://www.cochrane.org/about-us/our-policies/support-free-access-to-all-data-from-all-clinical-trials

Huberfeld, N. (2015). The Law and Policy of Health Care Quality Reporting. Georgia Journal of International and Comparative Law, 33(2), Retrieved from https://digitalcommons.law.uga.edu/gjicl/vol33/iss2/3/

Kolata, G. (2012, February 12). The Age of Big Data. The New York Times. Retrieved from https://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html

Woolley, S. C. (2011). The Measured Life. MIT Technology Review. Retrieved from https://www.technologyreview.com/2011/07/01/273518/the-measured-life/

Crawford, L. (2011). The Data Game. North Carolina Law Review, 88(1), Retrieved from https://scholarship.law.unc.edu/nclr/vol88/iss1/8/

Girion, L. (2011). Deadly Medicine. Vanity Fair. Retrieved from http://www.vanityfair.com/politics/features/2011/01/deadly-medicine-201101

Angell, M. (2004, July 15). The Truth About the Drug Companies. The New York Review of Books. Retrieved from http://www.nybooks.com/articles/archives/2004/jul/15/the-truth-about-the-drug-companies/?pagination=false

Dolan, B. (2015). Patients at Risk: The Need to Amend the Food, Drug, and Cosmetic Act to Ensure the Safety of Imported Prescription Drugs. Georgia Journal of International and Comparative Law, 33(2), Retrieved from https://digitalcommons.law.uga.edu/gjicl/vol33/iss2/3/

Stern, A. M. (2010, December 16). Audit Trails: The Corporate Surveillance We Need. Health Reform Watch. Retrieved from http://www.healthreformwatch.com/2010/12/16/human-farming-the-limits-of-medical-research/

Smith, R. (2003). Evidence Based Medicine. British Medical Journal, 326(7401), 1171. https://doi.org/10.1136/bmj.326.7401.1171

Hermann, R. C. (2016). Time and Money: An Analysis of the Legislative Efforts to Address the Prescription Drug Shortage Crisis in America. Retrieved from https://www.researchgate.net/publication/301501808_Time_and_Money_An_Analysis_of_the_Legislative_Efforts_to_Address_the_Prescription_Drug_Shortage_Crisis_in_America

Hirsch, F. (2005). End of the Line: The Rise and Coming Fall of the Global Corporation. New York, NY: Doubleday. N/A.

Brenner, S. W. (2012). Cloud Computing Providers and Data Security Law. Journal of Technology Law & Policy, 16(2), Retrieved from https://scholarship.law.ufl.edu/jtlp/vol16/iss2/2/

Noble, E. (2010). Big-Data Computing: Creating Revolutionary Breakthroughs. N/A.

Kansa, E. C. (2009). Enabling Reproducible Research: Licensing for Scientific Innovation. International Journal of Cultural Property, 16(3), Retrieved from https://ijclp.net/articles/abstract/10.5235/175799609789324540/

AllTrials. (n.d.). Retrieved from http://www.alltrials.net/

National Center for Biotechnology Information. (n.d.). The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. Retrieved from https://www.ncbi.nlm.nih.gov/books/NBK9576/#:~:text=The%20Health%20Insurance%20Portability%20and,Americans%20with%20health%20insurance%20coverage.

U.S. Department of Health & Human Services. (n.d.). Why is the Privacy Rule needed? Retrieved from https://www.hhs.gov/hipaa/for-professionals/faq/188/why-is-the-privacy-rule-needed/index.html

National Center for Biotechnology Information. (2017). Challenges in Electronic Health Records (EHR) Implementation: A Literature Review. Healthcare Informatics Research, 23(2), 73–82. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5171496/

National Center for Biotechnology Information. (2020). Electronic Health Records: A Review Comparing the Challenges in the United States and the United Kingdom. Healthcare Informatics Research, 26(4), 254–262. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7043175/#ref2

Li, Y. C., & Chou, Y. C. (2010). Electronic health records: What are the most important factors in achieving adoption? Journal of Medical Systems, 34(4), 379–384. doi:10.1007/s10916-010-9473-7

California Attorney General. (n.d.). California Consumer Privacy Act (CCPA). Retrieved from https://oag.ca.gov/privacy/ccpa

GovTrack.us. (n.d.). Congress Bills Statistics. Retrieved from https://www.govtrack.us/congress/bills/statistics

Massachusetts Attorney General. (n.d.). AG Reaches Settlement with Advertising Company Prohibiting Geofencing Around Massachusetts Healthcare Facilities. Retrieved from https://www.mass.gov/news/ag-reaches-settlement-with-advertising-company-prohibiting-geofencing-around-massachusetts-healthcare-facilities

Hunton, P. (2017, April 13). Massachusetts AG Settles Geofencing Case. Hunton Privacy Blog. Retrieved from https://www.huntonprivacyblog.com/2017/04/13/massachusetts-ag-settles-geofencing-case/#:~:text=On%20April%204%2C%202017%2C%20the,around%20women's%20reproductive%20healthcare%20facilities.

Predik Data. (n.d.). What is Geofencing Marketing and How to Use It. Retrieved from https://predikdata.com/what-is-geofencing-marketing-and-how-to-use-it/#:~:text=Geofencing%20marketing%20drives%20a%2020,based%20marketing%2C%20such%20as%20geofencing.

CurrentWare. (n.d.). Improve employee productivity: Monitor internet. Retrieved from https://www.currentware.com/blog/improve-employee-productivity-monitor-internet/#:~:text=Following%20a%20productivity%20analysis%20you,measuring%20productivity%20in%20the%20future.

Business of Apps. (n.d.). Health App Market. Retrieved from https://www.businessofapps.com/data/health-app-market/#:~:text=Health%20App%20Usage,-Calorie%20tracking%20app&text=In%20total%20there%20were%20560,increase%20from%20the%20previous%20year.

45 CFR Part 164 - Security and Privacy. (n.d.). Cornell Law School. Retrieved from https://www.law.cornell.edu/cfr/text/45/part-164/subpart-C

45 CFR § 160.103 - Definitions. (n.d.). Cornell Law School. Retrieved from https://www.law.cornell.edu/cfr/text/45/160.103

U.S. Department of Health & Human Services. (n.d.). HIPAA Security Laws & Regulations. Retrieved from https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

Google. (n.d.). Google's framework for responsible data protection regulation. Retrieved from https://services.google.com/fh/files/blogs/google_framework_responsible_data_protection_regulation.pdf

Statista. (n.d.). Lobbying expenses of Google from 2009 to 2020 (in million U.S. dollars). Retrieved from https://www.statista.com/statistics/277063/lobbying-expenses-of-google/

Center for Responsive Politics. (n.d.). Google Inc: Lobbying Profile, 2022. OpenSecrets.org. Retrieved from https://www.opensecrets.org/federal-lobbying/clients/summary?cycle=2022&id=D000067823

Hernandez, R. (2019, September 4). Google and other tech companies attempt to water down privacy law. Los Angeles Times. Retrieved from https://www.latimes.com/business/story/2019-09-04/google-and-other-tech-companies-attempt-to-water-down-privacy-law

Pew Research Center. (n.d.). Mobile fact sheet. Pew Research Center. Retrieved from https://www.pewresearch.org/internet/fact-sheet/mobile/

Nissenbaum, H. (n.d.). Privacy interests in public records. Retrieved from https://nissenbaum.tech.cornell.edu/papers/Privacy%20Interests%20in%20Public%20Records.pdf

Google. (n.d.). COVID-19 Open Data. Retrieved from https://health.google.com/covid-19/open-data/

Business of Apps. (n.d.). Health app market data. Retrieved from https://www.businessofapps.com/data/health-app-market/#:~:text=2023%20(%24mm)-,Health%20App%20Usage,that%20used%20them%20in%202021.

Google LLC. (n.d.). COVID-19 Google Mobility - BigQuery Public Datasets. Retrieved from https://console.cloud.google.com/marketplace/product/bigquery-public-datasets/covid19_google_mobility(cameo:browse)?filter=category:science-research&pli=1

Cuebiq. (n.d.). Location intelligence SaaS platform. Retrieved from https://www.cuebiq.com/press/location-intelligence-saas-platform/

ADP. (n.d.). Workplace monitoring: What's allowed, what's off limits. Retrieved from https://sbshrs.adpinfo.com/blog/workplace-monitoring-whats-allowed-whats-off-limits

Cuebiq. (n.d.). Retrieved from https://www.cuebiq.com/

Amazon Web Services. (n.d.). What is sentiment analysis? Retrieved from https://aws.amazon.com/what-is/sentiment-analysis/

American Red Cross. (2011, August 26). American Red Cross Shelter View App Makes Top 10 App List in iTunes Store [Press release]. PR Newswire. Retrieved from https://www.prnewswire.com/news-releases/american-red-cross-shelter-view-app-makes-top-10-app-list-in-itunes-store-128608623.html