The State of Health Data Privacy, and the Growth of Wearables and Wellness Apps

by

Joseph R. Krajcsik

Bachelor of Arts, University of Pittsburgh, 2015

Submitted to the Graduate Faculty of the

Graduate School of Public Health in partial fulfillment

of the requirements for the degree of

Master of Public Health

University of Pittsburgh

2022

UNIVERSITY OF PITTSBURGH

GRADUATE SCHOOL OF PUBLIC HEALTH

This essay was presented

by

Joseph Krajcsik

on

April 8, 2022

and approved by

Tina Hershey, JD, MPH
Associate Professor
Department of Health Policy
School of Public Health
Affiliated Professor
School of Law
University of Pittsburgh

Mary Crossley, JD
Professor of Law
School of Law
University of Pittsburgh
Co-Director of JD/MPH Program
School of Public Health

The State of Health Data Privacy, and the Growth of Wearables and Wellness Apps

Joseph R. Krajcsik, JD/MPH

University of Pittsburgh, 2022

Abstract

More than ever before, the capability for individuals to track and improve their own health is widely and publicly available. With wearable technology and wellness apps, a person can generate and study health data that before could only adequately be obtained by visiting a physician and undergoing tests. This technology also creates more ways for scientists, researchers, and health care providers to monitor and improve public health. Wearables and wellness apps however, despite their possible beneficial uses, are part of a growing trend in which more and more health information is being generated than can effectively be regulated. Many of the companies behind the technologies creating and capturing this data sit outside of HIPAA's purview, which only applies to entities that are providing health care services, transmitting health information for those services, or helping an entity to do so. In this largely unregulated space, wearable and wellness app companies have little restriction on what they can or cannot do with consumer data. While the European Union, as well as a small handful of States, have taken steps to regulate data privacy, the United States currently does not have an effective legislative scheme to regulate and protect the wide range of health data and information that these wearables and wellness apps are generating. To provide individuals with control over their own personal and health related information, the United States needs to create a legislative and administrative background that can adequately ensure consumer protection, while still fostering innovation and scientific research. To do so, the United States should mirror the European Union, and adopt a federal data privacy and

protection policy that creates a baseline standard that applies in every state. As part of this policy, individuals should be afforded more ownership and transparency with their own data, and privacy protections should be subject to the type of data itself, not the entity that is creating and/or processing it.

Table of Contents

List of Tables

1.0 Introduction

While physicians and health care workers ultimately provide healing, health advice, and specialized care, the lynchpin of these services relies primarily on something separate from their medical skills and knowledge – the trust that a patient has for their health provider. When a person discusses their health issues with a physician or health entity, they are sharing extremely private and intimate information. The protection of privacy in the healthcare community, and the maintenance of this aforementioned trust has been a core tenant since antiquity. To this day, the Hippocratic Oath has survived as a necessary pledge that physicians and healthcare workers adhere to (though now in a more modernized form) to ensure the confidentiality of their interactions with those they serve (Nass, Levit, & Gostin, 2009).[1] Without this trust, both individual and public sentiment turns against the medical community, evidenced by recent examples of anti-vaccination campaigns, anti-mask beliefs, and disillusionment with pharmacy companies. Much of that needed trust lies in the foundation of a confidential and private relationship, where information is not lost or shared to outside parties. Information however, collected in the form of data points, has expanded rapidly, particularly since the beginning of the COVID-19 pandemic. The "sacred" and private relationships that individuals traditionally had with their physician is slowly dwindling, in

[1] The Classical Version of the Hippocratic Oath is as follows: "I swear by Apollo Physician and Asclepius and Hygieia and Panaceia and all the gods and goddesses, making them my witnesses, that I will fulfill according to my ability and judgment this oath and this covenant . . . What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about" (Hippocrates, 400 B.C.E.).

a sense, as an evolving health sector, both utilizing and relying on innovation, has created bigger health organizations and bigger data collection. From a public health perspective alone, this essential data collection is used to monitor populations, prioritize resource allocation, and combat health threats (like COVID-19) – it's importance and use cannot be overstated (van Panhuis et al., 2014). Including individual healthcare, and the significant increase in health and wellness technology, our personal health related data is potentially in the care of a great number of organizations.

From a public health perspective, privacy is something that must be carefully balanced. The ideas of privacy and personal autonomy tie heavily into freedom and liberty. When these things are threatened, the public's trust in medicine and public health actions and interventions wavers, and it is much more difficult to effectuate positive change for the public's health. For society, health data needs to be protected. On the other hand, however, this very health data and the platforms that help create it, can be extremely useful to promote positive public health. The use of health data, wearable devices, and wellness apps has the ability to increase access to public health services, as well as help the public take their health into their own hands. Additionally, researchers and scientists use health data in many ways to understand and improve public health, and increased data privacy regulations create barriers to effective and efficient learning.

Policy-wise, it is in the best interest of the public's health to create a legislative and administrative background that can adequately ensure consumer protection of their health and health related data, while still fostering innovation and scientific research.

In some ways, the United States has already worked towards doing this. This privacy is so important that it has been protected under the law, both federally and at a state level. For example, federally, the Health Insurance Portability and Accountability Act (HIPAA) creates protections

and safeguards for a patient health information, while on a state level, the California Consumer Privacy Act (CCPA) greatly expanded a consumer's ability to take more control over their data privacy. These laws, however, are not as dynamic and quick to change as the industries and technology that they hope to regulate. Handwritten, paper files have given way to digital databases, and many of the largest companies in the world are in the business of collecting and selling that data. The general health privacy laws that have been enacted protect patient, or consumer data from being abused by those who are providing them traditional health services. Technology, and the business of data collection, has pushed companies that were outside of the healthcare sphere to offer consumers wellness services and monitoring, in which they have unregulated access to collect and use many of the same datapoints that health entities legally must protect.

Even when looking at the regulated health data that medical entities, legally termed "covered entities," and their business associates collect and use, theft and misuse still poses a significant threat. From 2005 to 2019, data breaches on the healthcare sector affected just under 250 million individuals, making it possibly the most targeted industry in the world for cyberattacks (Seh et al., 2020). In 2019 alone, the medical records of over 40 million people were either exposed or stolen (Seh et al., 2020). Due to personal health data largely consisting of static and unchanging information about a person, as opposed to credit information or internet passwords, which can be shut down or changed, health data can be up to twenty times more valuable on the illegal markets (TrapX-Labs, 2015). Even when this health data is not stolen by hackers, and simply collected by companies and health organizations, those with access have continuously been pushing the boundaries with how they use it, towing the line on the rights of privacy and fairness. This is particularly the case for organizations that are not currently subject to the enhanced privacy

requirements of HIPAA, as they have less limits as to what they can do with this personal, and oftentimes health-adjacent, data they collect.

1.1 Wearables and Wellness Apps and Their Place in Public Health

Two large and growing areas particularly fall within this unregulated region: wearables and wellness apps. Broadly speaking, wearables are devices that individuals can wear on (or have embedded or implanted within) their body that use sensors to generate, collect, and send information about the person wearing it, or even their surroundings. Popular examples of wearables include smart watches, tracking devices, smart glasses, and work-out monitors. Evolving technology within the space has allowed current wearables to generate and collect a broad spectrum of health and health related data.[2]

When used within healthcare and the public health field, the data generated and collected can help with making diagnoses, monitoring treatment, managing diseases, and following rehabilitation schedules. Outside of the traditional healthcare setting, these wearables can allow individuals to take more control over their own health, and act as also preventative, personalized self-care.

Similarly, wellness apps are mobile applications or platforms that are made for consumers and designed to promote healthier lifestyles. These privately owned and marketed applications are branded to cover the spectrum of personal, mental, and lifestyle health tracking. Almost all of these

[2] Including but not limited to: heart rate, oxygen saturation levels, hydration, blood pressure, geolocation (including elevation), general body motion, movement speed, stress, mood, and sleep information.

applications begin by requiring the consumer to create a user health profile, often prompting them to enter in personal and health related information such as age, height, weight, and location (this can be more specific depending on the wellness app design and intention). These apps exist largely outside of the healthcare context, and have seen a huge growth in use since the beginning of 2020. In April of 2020 alone, first time downloads of the top twenty mental wellness apps reached over 3 million, representing a 29% increase from January of 2020 (Herzog, 2020).

With so much personal health related information being entered into and captured by these devices, the question arises as to how companies are using this data. For example, increases in health tracking has led professional sports to be increasingly data driven, with players wearing tracking devices on and off the field. Recent collective bargaining agreements (CBAs) between player's unions and their respective leagues, has sought to address the collection and use of this data. In 2017, the NBA's new CBA outlined how data collected from wearable devices could be used, namely only for health and performance reasons related to on-court play; the CBA also explicitly stated that the data "may not be considered, used, discussed or referenced for any other purpose such as in negotiations regarding a future Player Contract" (Leung, 2017). Other professional leagues have similar restrictions on the use of player health data, such as the NFL and its protections on data obtained in voluntary "sleep studies" that track the sleeping habits of players (NFLMC & NFLPA, 2020). Similarly, other employers could use employee health data and insurance usage for decision making for possible terminations or job contract details (Lamberg,

2017).[3] As technological advancements in health care and technology increase, as well as hacking capabilities, the use and abuse of health data is only sure to get worse. The healthcare industry, due to their collection of data, most of which is personal health and identification information, is already a major target for hacking schemes. In 2015, health insurer Anthem Blue Cross Blue Shield suffered one of the worst data breaches in world history, when it was targeted and hacked by what was eventually deemed to be a Chinese based group (Riley, 2015). Over 78 million people had their personally identifiable information stolen, including things like their names, dates of birth, social security numbers, and even income data ("Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions, Including 2015 Data Breach of Health Insurer Anthem Inc. Affecting Over 78 Million People," 2019). Similar attacks occur on almost a daily basis, particularly ransomware attacks in which groups gain access to healthcare data and either steal it, or block access to it until a ransom is paid to them. These attacks increase every year, and it is estimated that from 2020 to 2025 the global healthcare cybersecurity market will spend up to $125 billion in attempts to prevent and limit hacking attempts (Morgan, 2020).

More and more, companies that are not subject to HIPAA's privacy and security requirements are entering into the wellness market, offering products that collect much of the same data that HIPAA would cover. Even with the aforementioned issues with health data in the regulated space, those regulations provide some level of assurance as to what data is being collected, where is going to, and how it is being used. These unregulated companies that have

[3] Lamburg discusses how hacked personal health data could reveal private information such as a person's sexuality and/or gender identity, which could be used for discriminatory purposes, and possibly lead to job termination or house eviction.

created wearables or wellness apps for consumer use do not have to adhere to these rules, and consumers have their own data and information sold to the highest bidder.

While these issues create a need for improved data privacy and security, wearables and wellness apps also present opportunities to improve the public's health, increase access, and possibly lower costs. Within healthcare, these technologies allow physicians to quickly receive patient data without the patient having to possibly travel to a faraway facility, or undergo invasive tests or procedures. Outside of healthcare, again, personal tracking of health and wellness can reduce future utilization of health services, in a sense allowing individuals to practice preventative medicine on themselves.

Balancing these potential harms and benefits leads to a series of questions that will need to be addressed as society ventures forward into an ever-digitalized world: what policies and legislation are necessary to ensure that the public's health data and information is properly protected and secure, while still allowing for it to be utilized to innovate and improve health? And more specifically, what even constitutes "health information" going forward? With the health community's recent push towards precision medicine and a focus on the social determinants of health, we now accept that health is affected by a vast litany of circumstances, and the line is getting more and more blurred as to what should and should not be covered and protected.

2.0 Legal Landscape

The idea of "health data" feels more intimate than other forms of data. A visit to a physician has always been one in which privacy is the prevailing theme. Patients are inherently vulnerable (especially when injured or ill) and the information being shared is done so within the confines of a particular, and, in a sense, sacred doctor-patient relationship. Increased data collection and use is quickly making any semblance of privacy a façade. The trust that that relationship relies upon, particularly when giving a provider with heath information becomes evermore important. A 2019 Pew Research study (n=4,272) looking into how Americans view the control they have over their personal information found that 62% of Americans believe that "it is not possible to go through daily life without companies collecting data about them" (Auxier et al., 2019). At this point in time, many consumers live under the presumption that their data is being collected and tracked, used in ways to manipulate or affirm our behavior and beliefs (largely for consumer purposes). While many may be against it, almost all individuals still carry a phone within their pocket that tracks their locations and their internet history. It is understand that social media platforms will use consumer data to try to make it difficult for a consumer to stop scrolling. Most consumers even accept, or ignore that when credit card information is entered online to purchase something, they might be taking a financial risk. But what can be done? Around eight out of ten Americans say they have "very little or no control over the data collected about them," are "at least somewhat concerned about how companies are using the data it collects about them," and believe that the "potential risks of companies collecting data about them outweigh the benefits (Auxier et al., 2019).

Largely, this entire field of information collection is minimally regulated. When it comes to information being collected within the healthcare field, and thus relating to this historically recognized doctor-patient relationship, policy-makers have shown, via the enactment of HIPAA, that allowing personal health data to be freely shared is a step too far. Despite this idea that personal health data might just be so sensitive that its privacy must be protected, the United States continues to have what is often referred to as a patchwork (and fairly uncomprehensive) legal scheme when it comes to protecting health data and privacy (Mulligan & Linebaugh, 2019). Federally, we began with HIPAA which was amended by HITECH, while on a state level there are varying enactments, the biggest and most pervasive being the CCPA. Adjacent to these legal frameworks, federal administrative agencies also have varying levels of enforcement over the protection of consumers, and thus make up a piece of this patchwork. For example, the Federal Trade Commission (FTC), through its Health Breach Notification Rule, imposes its breach notification requirements on entities not covered by HIPAA that are accountable for the loss of consumer sensitive health information. Very recently, the FTC decided to consider wellness apps, in certain situations, to be covered by this Rule, again incrementally extending this patchwork policy scheme (FTC, 2021).

2.1 Federal Action: Health Insurance Portability and Accountability Act (HIPAA)

HIPAA, enacted in 1996, was created to regulate and protect the maintenance and exchange of “protected health information”, or PHI, by covered entities (Bari & O'Neill, 2019). Before this, different states within the U.S. all had differing levels of privacy laws, requiring certain protections for specific types of information, in specific situations. As part of the Act, Congress also wanted to move towards a more standardized electronic form of documentation. Regulations were

promulgated to implement HIPAA, including the Privacy Rule, and the Security Rule. The Privacy Rule addresses the use and disclosure PHI by “covered entities,” as well as individuals’ privacy rights for how that information is used ("Summary of the HIPAA Privacy Rule," n.d.). It allows PHI to be shared when needed, but in ways that seek to ensure privacy. The Security Rule takes the protections of the Privacy Rule and specifies safeguards that “covered entities” have to put in place to protect the confidentiality, integrity, and availability of “electronic protected health information” (e-PHI) ("Summary of the HIPAA Security Rule," n.d.). The idea behind the Security Rule was to give a blueprint of flexibility for “covered entities” so they can continue to abide by the Privacy Rule and the rest of HIPAA within the inevitable shifts and innovations of the healthcare industry.

By carefully defining various terms and qualifiers, HIPAA frames specifically to whom, and to what it applies to.

Table 1: Major HIPAA Definitions

HIPAA Terms	Definitions
Covered Entity	Any health plan, health care provider, or health care clearinghouse (entity that converts non-standard health information into health data, or vice-versa) who transmits any health information in electronic form
Business Associate	Any person or organization with which a covered entity shares PHI in order for person or organization to perform a service for the covered entity
Protected Health Information	Any individually identifiable health information that is created, transmitted, or maintained by a covered entity or business associate and concerning past, current, or future condition, treatment or payment

Note. These definitions are paraphrased from HIPAA – 45 C.F.R. § 160.103 ("Health Insurance Portability and Accountability Act of 1996," 1996).

These definitions, taken together, establish that HIPAA applies to any entities that are providing health care services, transmitting health information in relation to those services, or helping such entities do so (because in such "helping" roles, they are likely to come into contact, posses, or transmit the health information as well). They are responsible for the privacy and security of "individually identifiable health information," which is further specified to apply to "information that is a subset of health information, including demographic information collected from an individual" ("Health Insurance Portability and Accountability Act of 1996," 1996). Apart from being created or received by a covered entity or business associate and relating to an individual's healthcare transaction with them, the information or data must identify the individual or do so to such an extent that there is a "reasonable basis to believe the information can be used to identify them" ("Health Insurance Portability and Accountability Act of 1996," 1996). Examples of this type of information include but are not limited to names, addresses, birthdates, social security numbers, phone numbers, emails, license plate numbers, and even biometric data. We see from this that some, but not necessarily all of the sort of information a wearable or wellness app may collect, would be covered if the entities owning or controlling those products were covered entities. These wearables and apps however, as discussed, are not regulated by these HIPAA requirements, so many can use the information in ways that they see fit.

Looking closely at the terminology only certain entities are subject to HIPAA's regulations. Companies that have now entered into the wellness industry, though they may offer services to help individuals count calories or track workouts, are not by definition involved in the provision

or payment of health care services. Thus, any of the data they collect, even if it is health or demographic information, falls outside of PHI.

Despite HIPAA's introduction of rules to govern e-PHI, the medical world's (as well as the rest of the modern world's) switch from paper filings to digital and electronic ones during the early 21st Century progressed slowly. To hasten this change, which would allow better access and treatment within health care, HIPAA was amended to include Information Technology for Economic and Clinical Health Act (HITECH) (Bui, 2016). HITECH, along with the later down the line Affordable Care Act (ACA), spurred the electronic adoption process through subsidies and financial incentives (Bui, 2016).

2.2 Health Information Technology for Economic and Clinical Health Act (HITECH)

Congress recognized that the essential shift to electronic records in the healthcare space, which allowed for more fluid and frequent record sharing, could create possible HIPAA-related security problems. In addition, there were gaps in HIPAA that allowed for misuse of PHI. For example, under HIPAA as originally enacted, business associates were technically required to comply with HIPAA, but their obligation was based on their contracts with covered entities, and they could not be punished directly. In 2009, Congress enacted the aptly named HITECH as a means to strengthen HIPAA. HITECH had a few key provisions that drastically affected how entities had to behave and respond to possible data security issues.

First, HITECH ensured enhanced enforcement by creating both mandatory, and increasing penalties for willful neglect, as well as stretching HIPAA's penalties to extend to business associates (Dahm, 2010). This hit business associates with a heavier burden, as they now had to

comply with the full extent of HIPAA's Privacy and Security rules; mandatory Business Associate Agreements were required, in which the third party associates agreed to comply with HIPAA and ensure PHI protection and security, or else face liability (Nahra, 2017).

Perhaps HITECH's biggest change related to the requirements entities must follow after a potential breach. If a possible breach was discovered, covered entities must now conduct a risk assessment to determine the extent and severity of the possible breach. If a significant breach is discovered, the covered entity has to, within 60 days, notify individuals whose PHI has potentially been accessed (Nahra, 2017). This provides individuals with greater control and notice over their PHI, while not allowing companies hide any major data breaches that they suffer. Until a recent FTC decision (discussed below), wellness apps and wearables could escape some of these requirements, and a breach that would impose obligations and conditions upon a covered entity or business associate would not always apply to the app company, despite possibly losing the exact same type of information.

There have been a handful of small, and largely underwhelming amendments to further push health privacy via HIPAA and HITECH since 2009. For example, the HIPAA Final Omnibus Rule of 2013 again put more onus on business associates, allowing them to be liable for lack of HIPAA compliance with or without a breach occurring. Aside from this change, little has been done within the law to protect the privacy concerns that have grown with the increased utilization of technology throughout the country. It has been over a decade since the HIPAA Final Omnibus Rule of 2013, and data creation and use has only exponentially increased. At the time that this move toward an electronic world spurred Congress towards enacting HITECH, health data and its abuse was only at its infancy. 2009 was the year that smartphones began to take off, and now, 12

years later data creation and collection occur on a scale likely unfathomable to many who helped push new legislation through.

2.3 The European Union's General Data Protection Regulation (GDPR)

Around the same that HIPAA was being discussed, the European Union entered into force their own privacy directive to respond to modern technological needs. The 1995 European Data Protection Directive set a floor for data privacy and security across Europe, allowing each member State of the EU to implement the requirements as they see fit. As technology advancements in almost all realms of life grew, and the prevalence of the internet and data collection became a part of everyday life, the European Parliament recognized a need for a more comprehensive approach on data protection that set a clear standard for all member states (Wolford, 2019).

The EU General Data Protection Regulation (GDPR), which came into force in May of 2018, gave EU citizens a right to their data, and effectively changed the landscape of privacy for the Europe. The GDPR applies to the processing or control of personal data (by a processor or controller) who is either: in the Union, or; is outside of the Union, but offers goods or services to data subjects in the Union, or monitors the behavior of those within the Union ("EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC," 2016). "Personal Data" is defined to mean "any information relating to an identified or identifiable [data subject]." This refers to anyone that can be directly or indirectly identified by almost anything. For example, the GDPR explicitly lists a series of broad health-adjacent identifiers that qualify, namely

ones that specifically refer to a person's "physical, physiological, genetic, mental, economic, cultural or social identity." "Processing" refers to any operation(s) performed on personal data, such as "collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." A processor is a person or organization that does this processing, while a controller is person or organization that "determines the purposes and means of" that processing ("EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC," 2016). With the powerful inclusion of the GDPR applying to any entity doing business in the EU, regardless of where the entity is located, the world was in effect forced to comply with its regulations.

The Directive works on seven key principles: lawfulness, fairness and transparency; minimalized purpose; accuracy; storage limitation and security; integrity and confidentiality; and, accountability. These seven principles are reflected in the specific rights that a data subject obtained with the GDPR.

Table 2: GDPR Rights

Rights Ensured by GDPR	What does this mean for the data subject?
Right to be informed	Data controller has to inform data subject about the collection and use of their personal data

Right of access	Data subject has right to request a copy of their data, as well as other information (e.g. purpose of processing, categories of data, etc.)
Right to rectification	Data subject has right to change or modify inaccurate personal data
Right of Erasure (Right to be forgotten)	Unless there are legitimate reasons for retaining the data, a data subject has the right to request the erasure of their personal data without undue delay
Right to restriction of processing	Data subject has right to restrict or impede processing of their data under certain conditions laid out in Article 18
Right to data portability	Data subject has right to request and receive their personal data and send it to another controller
Right to object	Data subject has right to object to data processing under certain conditions under Article 21
Right to not be subject to automated decision-making	Data subject has right to not be subject to decisions based solely on automated processing, such as profiling, which produces legal effects concerning them or significantly affects them

Note. These definitions are paraphrased from the EU GDPR, Ch. 3, Articles 12-22 ("EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC," 2016).

These rights work together to give data subjects ownership and control over their information, and information which could identify them. The GDPR attempts to create a privacy shield and data protection framework by "design and by default." Entities operating or conducting business in the EU are to create their products in such ways where privacy designed into them, and before options are given to consumers to consent to data sharing, the default mode is the most private. Wellness apps and wearables in the EU, due to this idea, can be fundamentally built with the protection of health and health adjacent information in mind; these companies would need to seek active consent from the consumer before information could be shared, sold, or even processed.

Besides consent, a processor or controller can only lawfully process personal data when there is a contractual necessity, a legal obligation, a legitimate and overriding interest, or to protect a data subject's vital interests, or the public's interest ("EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC," 2016). If an entity violates any of these rights, and processes data unlawfully, the GDPR allows for administrative fines, designed to ensure cooperation and discourage any poor data protection practices. While member states can implement additional penalties, the EU's maximum fine will be whichever is higher between

€20mm or 4% of global revenue ("FAQ," n.d.). Coupled with these possible hefty fines, compliance with the GDPR created a pretty large financial burden for entities, both relating to the creation of programs to ensure adherence, as well as the possible losses of millions of data subjects' personal data, which they may have been previously using for gain.

The GDPR's far-reaching protections for individuals in the EU and requirements for entities around the world inspired lawmakers to begin to follow in their footsteps in enacting privacy laws themselves. In the US, with little being done on a federal level, states have begun to enact laws that help to further secure health data and close loopholes that companies have been taking advantage of. Many of these enacted and proposed laws mirror the GDPR in some ways, though none are as broad-ranging and widely applicable.

2.4 State Action: California Consumer Privacy Act (CCPA)

Because HIPAA requirements apply only to a very specific set of covered entities, many companies have been able to enter the field of "health data collection" and use such data generally in any way they see fit. Data collected by wellness apps and smartwatches is beyond the reach of HIPAA as it currently sits. A study from 2019 found that, out of the 36 top-ranked publicly available apps for depression and smoking cessation, "29 transmitted data to services provided by Facebook or Google, but only 12 accurately disclosed this in a privacy policy" (Huckvale, Torous, & Larsen, 2019). Private data concerning tobacco usage or mental health history taken from applications such as these, can be packaged and sold to third-party vendors, many of whom use the data for targeted advertising. These wellness apps and products also collect a great deal of other information, which, on its face, may not be "health information" per se, but could at the very least

be called "health-adjacent information," as it is often the same sort of personal information HIPAA protects, or is more and more being used for health modeling and treatments. This health-adjacent information would include things such as geolocation tracking, income, education, age, etc.

Whereas HIPAA was enacted specifically to address security and privacy concerns surrounding PHI, governments are now broadening the scope and creating general privacy policies that provide protection and consumer ownership over personal and health-adjacent data. On a state level, in early 2018 California followed in the footsteps of the European Union in passing a comprehensive privacy act which among other things, largely prevents the harvesting of what is effectively individual health data, and protected health information. The California Consumer Privacy Act (CCPA), rather than creating protections based upon who the individual is, what company is obtaining it, and how they are doing so (like HIPAA and its reliance on a covered entity being involved), instead ties the protection to the data itself (Bari & O'Neill, 2019). [4] If the data point relates to qualified personal information, and the company receiving or creating it is subject to the provisions of the CCPA, it does not matter if they are a hospital or a car salesman.

When looking generally at what companies are subject to the CCPA, the law imposes its various requirements on "any business" that, among other things, collects the personal information of Californians or does business in California (Mulligan & Linebaugh, 2019). § 1798.140(d) of the CCPA defines a business as a for profit entity that collects consumer's personal information

[4] In late 2020 the CCPA was amended as the California Consumer Rights Act or "CPRA," which officially will come into effect in 2023. The CPRA expanded upon some of the consumer rights, as well as tweaked the thresholds and qualifiers for whether certain businesses fell under its purview, among other things. Any ensuing discussion of the CCPA includes the changes added by the CPRA.

(or broadly is involved with processing that consumer personal information), "does business in the State of California, [and] satisfies one or more of the following thresholds:

> (A) . . . had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year . . .
>
> (B) Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 100,000 or more consumers or households . . .
>
> (C) Derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information" ("CCPA," 2018a).

The law regulates any personal information, which in terms of data collection in the modern age, effectively means it regulates almost all data a business might receive from a consumer or individual. Furthermore, the CCPA drastically broadened how it sees "personal information" in comparison to HIPAA, with § 1798.140(v)(1) defining it as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household" ("CCPA," 2018b). This catch-all tells all companies who even consider doing business in California that they need to prepare themselves to be compliant with the CCPA, as there is not a clear way around it. Simply put, even though this is just a California law, it holds distinct sway—California is the most populous state in the United States and the global hub of technology.

In an effort to give consumers and individuals more control over their own information, the law instills the following privacy rights for Californians:

- The right to know;
- The right to delete;

- The right to opt-out;
- The right to non-discrimination ("California Consumer Privacy Act (CCPA)," 2022).

These rights tower over HIPAA when it comes to an individual's control over their own data, and fill in the gaps the federal privacy law leaves open. The right to know requires businesses to make available to requesting customers the categories of data that will be collected about them (before it is collected), what specific data is being collected, what categories of sources of information is the data acquired from, and the purpose of collecting their data ("CCPA," 2018b). Put more simply, businesses, if requested, have to give consumers the who, what, where, when and how on their data collection.

The right to delete to delete allows consumers to request their personal information to be deleted (though there are some exceptions, namely ones involving legal requirements or publicly available information) ("CCPA," 2018b).

The right to opt-out allows consumers to opt-out of the sale of their personal information ("CCPA," 2018b). While this is an active opt-out scenario, instead of a proactive opt-in one, businesses are required to clearly display a link that reads "Do Not Sell My Personal Information" on their website, and the process for requesting deletion has to be fairly quick and easy.

Lastly, the right to non-discrimination prevents a business from retaliating against a consumer for exercising their rights under the CCPA. Examples of this could include "denying goods or services to the consumer," or generally treating the consumer differently in terms of price or quality ("California Consumer Privacy Act (CCPA)," 2022).

The requirements imposed by the CCPA, GDPR, and HIPAA all put a large onus and responsibility on businesses to take active steps in ensuring they comply. With such a litany of

complex requirements, it may seem burdensome for businesses. However, it is necessary for consumer and patient privacy and safety.

What the CCPA importantly changed, as opposed to HIPAA, was the level of "identifiable." Both major pieces of legislation allow the selling or sharing of "de-identified" data. The CCPA used specific language to make that a greater bar to pass. Shown above, the Act's definition of personal information describes it as anything that can even be "*reasonably capable of being associated with*" a individual or *household*. This broader sense of association gives more leeway for the State to hold businesses accountable, and inclusion of "household" makes it so a particular individual need not even be identified; simply by sharing data that is linked to a household's IP address, a business can be violating the law.

2.5 State Action: Virginia and Colorado Follow California's Lead

Virginia was the first state to follow California's lead and pass their own comprehensive privacy law in early 2021, the Virginia Consumer Data Protection Act (VCDPA). A vast majority of the law closely mirrors the CCPA; however, there are a few distinctions. Colorado followed closely behind, passing the Colorado Privacy Act (CPA), which is almost a carbon copy of Virginia's law.

A lot of the difference in these three enacted laws are fairly nuanced, and apply in very particular circumstances. There are some major differences however, in who is subject to the laws, as well as enforcement methods.

To begin, California's law has the broadest scope. As stated above, the CCPA applies to a business that meets any of the three main annual requirements: makes over $25,000,000 in revenue

(revenue amount requirement); generates at least half of its revenue from selling or sharing Californian's data, or; buys, sells, or shares the personal information of over 100,000 Californians ("California Consumer Privacy Act (CCPA)," 2022). Virginia narrowed these requirements by removing the revenue amount requirement completely. The VCDPA, per § 59.1-572, only applies to businesses that either: control or process the personal data of at least 100,000 Virginians, or; control or process the personal data of at least 25,000 Virginians and generate at least 50% of its revenue from the sale of such data ("VCDPA," 2021).

Colorado's law on the other hand, is very similar to Virginia's, but instead of just targeting businesses that conduct business in their state, it also applies to any that intentionally target residents of Colorado; the CPA also lacks a revenue percentage requirement, applying to any qualified business that simply "derives revenue or receives a discount . . . from the sale of personal data and processes" ("Colorado Privacy Act," 2021).

Two more ways in the CCPA offers more breadth, is with its enforcement mechanisms and its exceptions. Though limited, the CCPA allows for a private right of action for those consumers whose personal information was subject to an unauthorized sharing or disclosure, or theft. Virginia and Colorado both lack this option, though in all three states, businesses violating these Acts are still subject to penalties ("CCPA," 2018b). All three of the statutes offer exceptions, where certain information or groups are not subject to the requirements. One such exception is for information that is publicly available. Broadly speaking, if the information is available to the public, it would be unnecessary for businesses either ignore it, or safeguard it to the level of private or protected information. California's law is stricter in its definition of "publicly available information," limiting it to information from records the government makes available, whereas Virginia and Colorado additionally include information that the business reasonably believes the consumer

lawfully made available to the public. Virginia spelled this out even more specifically, noting this would be done “through widely distributed media” ("VCDPA," 2021). This would allow businesses to take information made available through social media services, and use or sell it however they wish.

Lastly, it should be noted that all three states also include some sort of exception applying to some or all entities, or data that is already subject to HIPAA. Because these companies and this data is already regulated by HIPAA, it is unnecessary to impose these additional requirements on them, many of which are not as stringent or precise.

2.6 Other State Action Currently in Progress

The passage of these three landmark privacy laws has spurred legislators in a majority of U.S. states to introduce into Committee versions of their own. Many of these states have previously introduced similar policies, but oftentimes the bill would die in Committee or be postponed (Klosowski, 2021). For a bill to die in Committee, the proposed law was passed up, and legislators decided not to recommend it for a vote. This could occur for various reasons, some examples being that legislators could not decide or agree on the specifics within the law, or that other policy issues took a front seat and the bill was put aside for the time-being. After the successful passage of the three other state statutes, many newly introduced bills now have increased backing for implementation. This is coupled with the loosening of many restrictions, including consumer data and health data sharing ones, during the COVID-19 pandemic. By passing comprehensive privacy statues and policies, states can ensure that the successful parts of the easing of restrictions can stay, while ensuring that the data involved is adequately protected, and controlled more by the individual

themselves. There is a lot in common with these prospective statutes across the country, but they are far from identical. What can be seen, is that in most or all of them, there is at least some discussion over the basic rights and ideas that the CCPA brought into play.

Currently, four states have signed comprehensive consumer privacy bills into law: California, Colorado, Virginia, and Utah. Fifteen states, the vast majority of which are situated in the Northeast, actively have bills in committee.[5] The remaining states have either not had introduced a comprehensive privacy bill, or previously had, only for the bill to die within Committee.

When looking at the passed and currently under consideration bills, some rights that would be guaranteed to consumers appear to be more popular than others. For example, all of these bills include some form of the right of access to personal data, and the right to deletion (Lively, 2022). Legislators, and their constituents, seem to strongly want individuals to be able to know and see what companies are collecting about them, and even where that information may be going. The states do differ in a few key areas however, largely relating to how consent is viewed, and whether or not a consumer has a private right of action to get civil damages from a violating business. Most, but not all give consumers the right to opt-out. This is an affirmative decision that the consumer has to make, and as such, depending on how the specific requirements of the opt-out procedure play out, a consumer's data is allowed to be used by entities in certain ways until the consumer

[5] These states are: Alaska, Connecticut, Kentucky, Louisiana, Maryland, Massachusetts, Nebraska, New Jersey, New York, North Carolina, Ohio, Oklahoma, Pennsylvania, Rhode Island and Vermont.

actively takes steps to deny it.[6] This gives the individual more control, and if these states closely mirror what the CCPA and even some tech companies have been moving towards, the ease of opting-out will be such that consumers are asked at the outset of using a product or wellness app whether or not they consent to having their data tracked and processed.

The vast majority of these bills also create obligations for businesses mirroring the EU GDPR's purpose requirements, in which the collection and processing of personal data is restricted unless done for a specific purpose (Lively, 2022). This restriction, however, does not adequately address the issue as to what sort of information should be allowed to be collected, shared and sold. Health adjacent information could in many states still be used in ways that normally would be disallowed should the entities and processors creating and using that data be subject to HIPAA. How can privacy policy ensure the practice of data minimalization, so that companies are restricted to collecting only the data they need to provide an offered, while simultaneously not hindering innovation and beneficial research? This all leads further down toward the issue that was proposed earlier, involving what should now be considered protected health information?

[6] As to the opt-in/opt-out variations, it is important to note that almost all states have some sort of age restriction built into their privacy bills, in which consumers that are minors (states vary on whether this applies to those under 13, 16, or 18) have to opt-in to allow the sale of their personal information.

3.0 Issues Going Forward in an Ever-Digital World

This current state-by-state privacy law system, coupled with HIPAA's stringent, yet narrowly tailored health information privacy framework, has created a patchwork legal system that is trying to protect individual's personal health data in a world that every day becomes more data driven. As mentioned above, many Americans already believe that we live in a society where the idea of privacy is unheard of it and rarely ever experienced. Health technology has been adapted to points in which we can take information about people, not previously before considered related to health, and create treatment plans, predictive health analyses, and potential public health interventions. Similarly, technology advancements have allowed the wellness industry to flourish and grow, as individuals seek convenient and simple ways to stay healthy, track their lifestyles, and monitor their bodies. Wearables, most commonly now in the form of smart watches, have developed to the point where technology companies are able to collect health and wellness information in the form of heartrate, oxygen levels, electrocardiograms, sleep schedules, hydration levels, and other geolocation-based data points. While it is wonderous that all of things are possible, and ultimately allow individuals to potentially gain better access and care, there is the potential tradeoff of that information being used by those companies. With growth within the industries, privacy questions are becoming more and more relevant.

3.1 Wearable Technology and Wellness Apps and Privacy

As of June, 2019, 21% of adults in the United States responded that they "regularly wear a smart watch or wearable fitness tracker" (Vogels, 2020). With wearables becoming more and more advanced, connecting with both our phones and our homes, it would not be a surprise if that number increases in the coming years. These devices, even when speaking only about the consumer products made by the Apples, Garmins, and FitBits of the world, are used to track and record numerous data points that most would consider health information (Vogels, 2020). All of this data is shared with the company who makes the wearable product, and largely they are able to share this information with third-parties and targeting advertising companies. Generally, HIPAA would require the transmission of this PHI to be encrypted, secure, and private, but because the individual using the product is not a patient receiving any health care services from a covered entity, HIPAA falls short of regulating this data collection and transmission (Bui, 2016).

Even if these companies worked to make the data given out anonymous and non-identifiable, technology and machine learning is at such a point that re-identifying information, especially when as personal as a person's location and heartbeat, is not out of the question.

Similarly, wellness and fitness apps sit in this same unregulated space, collecting health-adjacent information, and growing fast. As of July 2020, around 86 million Americans used wellness apps, a number purported to grow rapidly over the COVID-19 pandemic as many were kept indoors and away from more traditional health and fitness centers. While not solved in a greater protection way, this issue was at least recognized by the Federal Trade Commission (FTC) in late 2021. The FTC, whose mission is to protect consumers from unfair or deceptive business practices, oversees general data security breaches, and has strong breach notification requirements for U.S. businesses. One such previous rule, the Health Breach Notification Rule, "ensures that

entities not covered by HIPAA face accountability when consumers' sensitive health information is breached" (FTC, 2021). In a policy statement, the FTC noted that wellness apps are increasingly collecting health data, and have not been responsible in many ways for breaches. Recognizing this, the FTC decided that they consider wellness apps to be covered by the Rule if they are capable of drawing information from multiple sources, and "are not covered by a similar rule issued by the Department of Health and Human Services. What this means is the government is now subjecting wellness apps that are normally not covered by HIPAA (or another rule) to their breach notification rules if their app can, for example, combine consumer inputs with their fitness tracker, or if their app takes health information from one source (such as oxygen levels or weight) "but also takes non-health information from another source (e.g., dates from your phone's calendar)."

While this is a great first step, health-adjacent information may not be included, and the Rule only applies should health information be breached, forcing the company in question to notify consumers of the breach. Additional steps, codified more heavily into law than this administrative policy statement, are needed to protect consumer health, and health-adjacent information from misuse and abuse.

From a policy perspective, we want to protect consumer health and health related data from being improperly protected, or shared indiscriminately for purposes which are not beneficial to the individual whose data is being used. In doing so, we would allow these individuals to gain a greater ownership interest in their own data. At the same time however, policy changes like the one the FTC made need to be carefully thought out, as it would be bad public health policy to incidentally hinder innovation in the wearable and wellness app space, as these products, when used correctly and securely, benefit individual and public health. In the same vein, we want to ensure that researchers and scientists who rely on what is largely protected health data to perform their work

are not effectively locked out via strict and cumbersome regulatory requirements that may be difficult for them to meet.

The future of health care revolves around this sort of new and innovative technology. In this data driven world, how can we balance innovation and personalized care, with data safety and protection?

4.0 Possible Policy Solutions

As the U.S. moves forward into this data controlled and sold world, strong and comprehensive federal laws must be established to bring clarity to the current patchwork legal framework. The present trajectory of fifty states establishing fifty different privacy standards to protect health and health adjacent information, though a step in the right direction, could lead to such a confusing and complex web of regulations that compliance becomes difficult to achieve. This would in turn lead to individuals in different states having completely different levels of control over their own data, or even their data being misused and abused, as companies struggle to maintain the proper protections. Ultimately, a blanket federal policy standard would be much easier to both implement and understand for businesses, compared to having to have a different set of policies for each state they are or even might operate in. It would also avoid having the issue where individuals living in one state have comprehensive health data privacy, while their neighbor in another state have little control over how their own data is being used. This baseline federal policy would be similar to what the EU did, as it sought to correct its own patchwork and fragmented privacy protections. To companies and businesses, such a change would allow them to know exactly what is required of them, without having to juggle setting up fifty different compliance teams.

Politically, such legislation has been introduced and debated, largely with bipartisan support. In 2018 the Trump Administration spoke of implementing an "outcome-based approach," rather than mandating long and detailed rules (Mulligan & Linebaugh, 2019). The desired outcomes were: transparency, control, reasonable minimization, security, access and correction, risk management, and accountability (Mulligan & Linebaugh, 2019). While these are respectable

"outcomes," which in sense mirror the "rights" that states have developed, the Trump Administration failed to offer much of a plan as to how they would be achieved, and ultimately the outcome-based approach idea seems to rely too much on data collectors to police themselves, rather than adhere to stringent rules.

In mid-2019, Senators Klobuchar and Murkowski worked across the aisle to introduce the Protecting Personal Health Data Act, which would specifically provide new rules for technologies that collect personal health data such as wearables and genetic testing services. While not nearly as expansive as the later CCPA, the bill, which was referred to the Committee on Health, Education, Labor and Pensions, does seek to create federal rights to delete and amend health data (Tonsager, Kraus, Ackerman, & Ponder, 2019). Another Act was re-introduced in March of 2021 (the Cyber Shield Act), which primarily would create a cybersecurity certification program for "Internet of Things" devices, meaning internet connected devices, which would broadly strengthen the protections given to health adjacent information (Miller, 2021).

These various solutions all have things to like about them, but they suffer from attempting to fix the issue, rather than getting ahead of it. Continued incrementalism and half-measures will not be able to keep up with the growth of data collection and usage, specifically for health data. In truth, it may very well be impossible to get ahead of technology, and create a regulatory scheme that adequately covers future innovation. This impossibility however, provides all the more motive for acting now to attempt to gain some control, rather them employing an incremental and reactionary approach.

The United States should work to get ahead of this pervasive issue, and follow in the EU and California's footsteps, giving the people back control over their own data which they produce. This should be done by doing a few things. Currently, under HIPAA, individually identifiable

health information is only protected when it is created by or involved with a covered entity; individually identifiable health information should fall under similar definitions to those that the CCPA uses, in which the consumer is protected by the existence of their consumer health data, not by the data's relation to a specific entity. This need not even be done in a sweeping legislative act, such as the GDPR, but could be expanded upon via an amendment to HIPAA itself. For example, HITECH was able to extend HIPAA requirements to more effectively enforce upon, and apply to business associates, so a similarly intentioned amendment could be created to extend HIPAA requirements even further to any entity involved in the collection, sharing, or use of PHI or PHI related data, regardless of their direct interaction with healthcare providers. A change such as this would ensure that when a wearable or wellness app is collecting information that is either directly health related, or being used for a health motivated purpose, the companies involved must adhere to the regulations that would apply any covered entity that collected the same information.

Secondly, the U.S. should on a federal level ensure that individuals have the major rights the CCPA and GDPR have: rights to information and knowledge about your data, rights to access it, rights to erase it, and rights to restrict it. These rights would allow individuals to take more control over their own data. Among those rights would be requirements in which companies would be required to be transparent as to how your data will be used, and who it will be given to. In addition to this, like how HIPAA currently limits its scope to covered entities, federal policy could limit the scope that data collection companies are allowed to have. It could be possible to limit the amount of health information that is being collected, effectively capping it, or possibly less controversial, limit how companies are allowed to use the health-related data they obtain. Uses could have to be ethical, and related to improving the public or individual health, which would restrict the blanket selling for advertising or other purposes.

There are limitations in the potential measures that could be introduced, which warrant discussion. The general theme of many of the state promoted data privacy acts focuses heavily on notice and consent when it comes to data protection. While it does give consumers the requisite knowledge that their data is being collected and used, or even the option for them to either opt-in or opt-out, does allowing a person to click yes on a box on their computer or phone really give them more control? Also, as we have seen with health adjacent information, it is difficult to predict how certain disclosures of information might be able to be used in the future.

Another major hurdle affecting health data privacy relating to increases in recent technology deals with policies focusing solely on information that is identifiable. A great deal of health information becomes "de-identified," and mostly falls outside of the coverage of the laws. Researchers however, are finding that given current publicly available information and artificial intelligence systems, it is much easier to re-identify this information. These artificial intelligence systems are able to work through and analyze data sets to quickly identify correlations and patterns that allow for predictive analyzes and assumptions to be made. For example, a 2018 study looked at de-identified hospital discharge data from Maine and Vermont, and was able to successfully, using only newspaper articles and reports, re-identify 28.3% of the Maine individuals, and 34% of the Vermont individuals; the hospital data was then redacted to fully match the HIPAA standards, and the Maine data allowed for 3.2%, while the Vermont data allowed for 10.6% reidentification rates (Yoo, raThaler, Sweeney, & Zang, 2018).

Similar studies have had increased success using other publicly available information, such as voting records. This brings to light the issue that de-identification standards need to be adapted to combat the increased ability of tech and AI to successfully re-identify individuals whose protected health information is being sold and shared.

5.0 Conclusion

By giving individuals the ability to choose to control their own data, and doing so on a federal level, we can ensure that companies are more responsible with how they use health data and information. Essentially, this issue involves the internet, which is too pervasive and widespread to be wielded differently in each state. With California already leading the way, other states are sure to follow in some version or another, and businesses across the country would be much harder pressed to attempt to ensure they comply with fifty different privacy policies, rather than one comprehensive and transparent one.

Currently, there appears to be a window of opportunity in which action on this issue could be successfully implemented. There appears bi-partisan support, which matches what the public feels. Similarly, the timing of the COVID-19 pandemic set the stage for change to occur, both in the form of ability, and need. Throughout the pandemic, both individuals and businesses were forced to pivot even more quickly into a reality in which technology plays a role in almost every portion of life. Policy changes to create greater privacy requirements would likely be less detrimental for entities to implement, as many of these companies have had to update or create a cybersecurity and technology portion of their business. Similarly, COVID-19 has brought to light the importance of being able to use public health information to promote population health and security. With regulations in place to provide greater protection for individuals, in theory possible trust issues involving the medical and research community would be lessened. Innovation in personal wearable health and wellness is not stopping. Now is the time to take a major step towards protecting ourselves and our future.

Bibliography

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*. Retrieved from https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf

Bari, L., & O'Neill, D. P. (2019). Rethinking Patient Data Privacy In The Era Of Digital Health. Retrieved from https://www.healthaffairs.org/do/10.1377/forefront.20191210.216658

Bui, J. (2016). Lack of Privacy Regulations in the Fitness and Health Mobile App Industry: Assessing the Health Insurance Portability and Accountability Act (HIPAA) for Meeting the Needs of User Data Collection. *University of San Francisco Intellectual Property and Technology Law Journal, 21*(1).

California Consumer Privacy Act (CCPA). (2022). Retrieved from https://oag.ca.gov/privacy/ccpa

California Consumer Privacy Act of 2018, § 1798.140(d), 1798.100 Stat. (2018a 06/28/2018).

California Consumer Privacy Act of 2018, § 1798.140(v)(1), 1798.100 Stat. (2018b 06/28/2018).

Colorado Privacy Act, § 6-1-1301, et seq. , 6-1-1301 Stat. (2021 07/08/2021).

Dahm, L. L. (2010). Carrots and Sticks in the Hitech Act: Should Covered Entities Panic? *The Health Lawyer, 22(6)*.

EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, L 119 C.F.R. (2016).

FAQ. (n.d.). Retrieved from https://gdpr.eu/faq/

FTC. (2021). *Statement of the Commission*. (P205405). https://www.ftc.gov/news-events/news/press-releases Retrieved from https://www.ftc.gov/legal-library/browse/statement-commission-breaches-health-apps-other-connected-devices

Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 § 264 (1996 09/21/1996).

Herzog, K. (2020). Mental health apps draw wave of new users as experts call for more oversight. Retrieved from https://www.cnbc.com/2020/05/24/mental-health-apps-draw-wave-of-users-as-experts-call-for-oversight.html

Hippocrates. (400 B.C.E.). The Oath (F. Adams, Trans.). In. http://classics.mit.edu/index.html: MIT.

Huckvale, K., Torous, J., & Larsen, M. E. (2019). Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation. *JAMA Netw Open, 2*(4), e192542. doi:10.1001/jamanetworkopen.2019.2542

Klosowski, T. (2021). The State of Consumer Data Privacy Laws in the US (And Why It Matters). Retrieved from https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

Lamberg, A. (2017). Hackers Made Me Lose My Job!: Health Data Privacy and Its Potentially Devastating Effect on the LGBTQ Population. *Golden Gate University Law Review, 47*(2). Retrieved from https://digitalcommons.law.ggu.edu/ggulrev/vol47/iss2/10

Leung, D. (2017). NBA Teams Banned from Using Wearables Data in Contract Negotiations, Player Transactions. Retrieved from https://www.si.com/media/2017/02/02/nba-data-analytics-new-cba-wearable-device.

Lively, T. K. (2022). US State Privacy Legislation Tracker. Retrieved from https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions, Including 2015 Data Breach of Health Insurer Anthem Inc. Affecting Over 78 Million People. (2019). [Press release]. Retrieved from https://www.justice.gov/opa/pr/member-sophisticated-china-based-hacking-group-indicted-series-computer-intrusions-including

Miller, M. (2021). Lawmakers reintroduce legislation to secure internet-connected devices. *The Hill*. Retrieved from https://thehill.com/policy/cybersecurity/544711-lawmakers-reintroduce-legislation-to-secure-internet-connected-devices/?rl=1

Morgan, S. (2020). Healthcare Industry to Spend $125 Billion on Cybersecurity from 2020 to 2025. Retrieved from https://cybersecurityventures.com/healthcare-industry-to-spend-125-billion-on-cybersecurity-from-2020-to-2025/.

Mulligan, S. P., & Linebaugh, C. D. (2019). *Data Protection Law: An Overview* (CRS Report for Congress, R45631). Retrieved from https://www.hsdl.org/?view&did=823585

Nahra, K. (2017). The Past, Present and Future of Health Care Privacy. In *The Health Law Handbook* (2017 ed. ed.): Thomson Reuters.

Nass, S. J., Levit, L. A., & Gostin, L. O. (2009). Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research. In S. J. Nass, L. A. Levit, & L. O. Gostin (Eds.), *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research* (2 ed.). Washington (DC).

NFLMC, & NFLPA. (2020). *Collective Bargaining Agreement*.

Riley, C. (2015). Insurance Giant Anthem Hit by Massive Data Breach. Retrieved from https://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/.

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare Data Breaches: Insights and Implications. *Healthcare (Basel), 8*(2). doi:10.3390/healthcare8020133

Summary of the HIPAA Privacy Rule. (n.d., 07/26/2013). Retrieved from https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

Summary of the HIPAA Security Rule. (n.d., 07/26/2013). Retrieved from https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

Tonsager, L., Kraus, A. D., Ackerman, W., & Ponder, J. (2019). Legislation Seeks to Regulate Privacy and Security of Wearables and Genetic Testing Kits. *Inside Privacy*. Retrieved from https://www.insideprivacy.com/data-privacy/legislation-seeks-to-regulate-privacy-and-security-of-wearables-and-genetic-testing-kits/

TrapX-Labs. (2015). *Anatomy of an Attack: Medjack (Medeical Device Hijack)*. Retrieved from https://securityledger.com/wp-content/uploads/2015/06/AOA_MEDJACK_LAYOUT_6-0_6-3-2015-1.pdf

van Panhuis, W. G., Paul, P., Emerson, C., Grefenstette, J., Wilder, R., Herbst, A. J., . . . Burke, D. S. (2014). A systematic review of barriers to data sharing in public health. *BMC Public Health, 14*, 1144. doi:10.1186/1471-2458-14-1144

Virginia Consumer Data Protection Act, Title 59.1 § 59.1-572 (2021 03/02/2021).

Vogels, E. A. (2020). *About one-in-five Americans use a smart watch or fitness tracker*. Retrieved from https://www.pewresearch.org/fact-tank/2020/01/09/about-one-in-five-americans-use-a-smart-watch-or-fitness-tracker/

Wolford, B. (2019). What is GDPR, the EU's New Data Protection Law? Retrieved from https://gdpr.eu/what-is-gdpr/

Yoo, J. S., raThaler, A., Sweeney, L., & Zang, J. (2018). Risks to Patient Privacy: A Re-identification of Patients in Maine and Vermont Statewide Hospital Data. *Technology Science*. Retrieved from https://techscience.org/a/2018100901/