VOLUME 4 September 2023 ISSUE 2

JOURNAL ON EMERGING TECHNOLOGIES

© Kali Peeples

## NOTES

# A SLEEPING GIANT: MHEALTH APPLICATIONS, THE GDPR, AND THE NEED FOR FEDERAL PRIVACY REGULATION IN THE UNITED STATES

*Kali Peeples*



Individuals and nonprofit institutions may reproduce and distribute copies of this article in any format, at or below cost, for educational purposes, so long as each copy identifies the Author, provides a citation to the *Notre Dame Journal on Emerging Technologies*, and includes this provision and copyright notice.

# A SLEEPING GIANT: MHEALTH APPLICATIONS, THE GDPR, AND THE NEED FOR FEDERAL PRIVACY REGULATION IN THE UNITED STATES

*Kali Peeples**

## INTRODUCTION

The creation and evolution of the smartphone has ushered in a technological marvel that is a double-edged sword: mobile health applications (mHealth apps).[1] While this digitized tool enables people to access healthcare from the palms of their hands to track potentially life-threatening ailments or other health-related concerns,[2] mHealth also necessitates the uploading of personal information to online databases that are ripe with privacy issues. As mHealth becomes more integrated within society and healthcare, it is imperative to highlight how privacy legislation from around the world is aiming to combat these issues to create a safe environment for consumers. An analysis of privacy regulation concerning mHealth apps is a multifaceted process that requires the examination of changes within not only the healthcare space but also the technological world, as well as the legislative history and intent of various nations.

Part I focuses on the development and rapid creation of mHealth apps within the past decade. Part II seeks to illustrate the distinct privacy

---

* Juris Doctor Candidate, Notre Dame Law School, 2024; Bachelor of Arts in Biology and Africana Studies, Bucknell University, 2021. Many thanks to Professor Sadie Blanchard for her guidance and encouragement as my advisor for this Note, and to my colleagues on the *Notre Dame Journal on Emerging Technologies* for their hard work in editing and providing feedback for this piece. I also want to express my sincere love and appreciation to my family and friends. Thank you for your continuing support throughout my law school journey.

[1] Barbara Fox, *Mobile Medical Apps: Where Health and Internet Privacy Law Meet*, 14 HOUS. J. HEALTH L. & POL'Y 193, 193 (2014); *see also* Anne Marie Helm & Daniel Georgatos, *Privacy and MHealth: How Mobile Health "Apps" Fit into a Privacy Framework Not Limited to HIPAA*, 64 SYRACUSE L. REV. 131, 134 (2014) ("mHealth occurs when a provider of healthcare services uses connected and interactive mobile computing to produce, access, transmit, or store data for the provision of healthcare services to patients, or when a patient or consumer uses connected and interactive mobile computing to produce, access, transmit, store, or otherwise share data for a health-related purpose.").

[2] David Smahel, Steriani Elvasky & Hana Machackova, *Functions of mHealth Applications: A User's Perspective*, 25(3) HEALTH INFORMATICS J. 1065, 1065 (2017).

concerns of mHealth apps by concentrating on the evolution of the physician-patient dynamic and the digitalization and personalization of healthcare. Once the privacy issues of mHealth are illustrated, this piece turns to privacy legislation from multiple countries that aim to combat these concerns. Part III concentrates on the current American piecemeal approach of having federal acts and state-specific privacy laws to protect American consumers. As this deficient approach does not account for the vast array of different types of mHealth apps, nor the plethora of information that each app gathers, Part IV looks towards Europe for a potential solution. This part details the European Union's General Data Protection Regulation and how this regulation assigns extra protections and privileges to sensitive health data. As European Union countries can enact stricter provisions where the General Data Protection Regulation falls silent, Part IV also examines Germany's conservative approach regarding health data privacy protections, as well as Finland's liberal approach.

The main issue being addressed in this paper is whether the United States should create nationwide legislation that directly relates to mHealth data protection or continue with a self-regulatory method. Part V illustrates the pros and cons of each argument to determine which approach will sufficiently address American consumers' concerns surrounding the protection of their health data. Ultimately, this piece argues that the United States should create legislation that resembles the European Union's General Data Protection Regulation to account for the rapidly evolving technological world.

## I. THE EVOLUTION OF DIGITAL HEALTHCARE AND MHEALTH APPS

Technology, especially through the use of smartphones, has become embedded in almost every individual's life. From 2010 to 2016, the use of smartphones within the United States increased from 35% to 77%.[3] In 2020 alone, over 90,000 mHealth apps were created and developed for online stores, totaling to an average of almost 250 new mHealth apps every day.[4] By 2021, there were more than 300,000

[3] Aisha T. Langford, Craig A. Solid, Ebony Scott, Meeki Lad, Eli Maayan, Stephen K. Williams & Azizi A Seixas, *Mobile Phone Ownership, Health Apps, and Tablet Use in US Adults with a Self-Reported History of Hypertension: Cross-Sectional Study*, 7(1) JMIR MHEALTH & UHEALTH 1, 2 (2019).

[4] Emily May, *How Digital Health Apps are Empowering Patients*, DELOITTE (Oct. 19, 2021), https://www2.deloitte.com/us/en/blog/health-care-blog/2021/how-digital-health-apps-are-empowering-patients.html.

mHealth apps available on online stores.[5] While many apps were initially created to help monitor chronic health conditions, such as diabetes, obsessive-compulsive disorder (OCD), post-traumatic stress disorder (PTSD), and obesity, a significant boom in the mHealth industry came from the development of applications focused on preventative care, such as dieting and fitness.[6]

Now, mHealth apps can be split into two categories: consumer apps and provider apps.[7] Consumer apps can be characterized as health and wellness apps that are "designed for consumers who want to track and/or analyze their health on a personal level;" this includes apps that "support diet and exercise programs, reference aids, symptom checkers, and self-diagnostic tools, as well as those with more specific functions like pregnancy trackers and sleep-and-relaxation aids."[8] Provider apps are mHealth apps that are specifically related to medical providers, and these apps relay information about clinical decisions, patient diagnoses, treatments, and remote patient monitoring to both the medical professionals and their patients.[9] The multitude of mHealth apps that have flooded online markets has had a profound effect on not only people's relationships with technology and their doctors, but also on doctors', and potentially app developers', responsibilities and duties to their clients and consumers.

## II. MHEALTH AND PRIVACY CONCERNS

Privacy is an ever-changing legal space that evolves not only with time but also with the development of new technologies. Legal scholars and law makers have struggled with protecting the privacy of individuals as privacy covers a wide range of issues that cannot simply be fixed by a "one size fits all" solution; rather, as leading privacy scholar Daniel J. Solove suggests, it is imperative to acknowledge specific privacy concerns of a given field and address them directly.[10] For mHealth, there are six specific privacy concerns: (1) surveillance through the collection of information by either "overt or secret means";[11] (2) improper protection of sensitive information by digital security lapses or illicit use of

---

[5] *Id.*; *see also* Trix Mulder, *Health Apps, Their Privacy Policies and the GDPR*, 10 EUR. J. L. & TECH. 1, 2(2019).
[6] Fox, *supra* note 1, at 195-96.
[7] Helm & Georgatos, *supra* note 1, at 137-38.
[8] *Id.*
[9] *Id.* at 138.
[10] Daniel J. Solove, *A Taxonomy of Privacy*, 153 U. PENN. L. REV. 477, 481 (2006).
[11] Helm & Georgatos, *supra* note 1, at 139.

information;[12] (3) identification of private information to specific individuals;[13] (4) unsanctioned secondary use (when collected information is used for an unknown and unauthorized purpose);[14] (5) aggregation of small bits of information that ultimately add up to a holistic medical record;[15] and (6) disclosure of "true but sensitive information."[16] These six privacy points can be summarized by a conclusion with two key contentions: mHealth privacy concerns relate to the *sensitive nature of the data* being analyzed and the means by which this data is *collected, processed, and disseminated*.[17] While these concerns about the handling of sensitive medical data have been addressed in the past through the oaths of medical professionals and the standardization of medical treatment, technology has caused these checks to become obsolete. Thus, to understand why a sound and cohesive privacy regulation is needed for mHealth apps, it is crucial to understand how the healthcare landscape has changed.

### *A. Protection of Sensitive Information and the Hippocratic Oath*

Created in the fourth century, and continued to be used today,[18] the Hippocratic Oath is the main vehicle by which a doctor vows to protect the confidentiality and privacy concerns of their patients.[19] This oath has become a foundational element in numerous codes of ethics,

---

[12] *Id.* at 139-40.
[13] *Id.* at 140.
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] *Id.* at 139.
[18] A modern rendition of the Hippocratic Oath states, "I will respect the hard-won scientific gains of those physicians in whose steps I walk, and gladly share such knowledge as is mine with those who are to follow . . . *I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know* . . . . I will remember that I do not treat a fever chart, a cancerous growth, but a sick human being, whose illness may affect the person's family and economic stability. My responsibility includes these related problems, if I am to care adequately for the sick . . . . May I always act so as to preserve the finest traditions of my calling and may I long experience the joy of healing those who seek my help." Louis Lasagna, *The Hippocratic Oath: Modern Version*, PBS NOVA, https://www.pbs.org/wgbh/nova/doctors/oath_modern.html (last visited Jan. 21, 2023) (emphasis added).
[19] Mark Rothstein, *The Hippocratic Bargain and Health Information Technology*, 38(1) J. L. MED. ETHICS 7, 7 (2010). *But see id.* (cautioning that, while the Oath aims to protect privacy concerns, ancient Greece had different notions of privacy as "[p]hysicians took histories, examined patients, gave prognoses, and practiced surgery in public or in houses as relatives and strangers looked on").

including the 1984 American Medical Association's code of ethics.[20] According to scholar Mark Rothstein, the Oath establishes a type of "bargain;" this bargain can be summarized as:

> Allow me to examine you in ways that you would never permit any stranger, and tell me the most sensitive information about your body, mind, emotions, and lifestyle. These intrusions upon your privacy are essential in providing you with sound medical care. If you provide me with this intimate access to your person, I promise to maintain your secrets for as long as I live and to disclose them only if directed by you or others you have authorized.[21]

The Hippocratic Oath, and thus this bargain, has rapidly evolved throughout the years. What has initially started out as a physician-patient relationship that consisted solely of one healthcare practitioner has evolved into a type of patient care that involves a diverse array of medical professionals from numerous specialties in order for individuals to receive proper medical treatment.[22] Now, a concern about having a sole practitioner knowing a person's medical ailments has transmogrified into having multiple individuals, including but not limited to technicians, laboratory and pharmacy staff, physical therapists, and other specialists, being involved in a patient's treatment, thereby subjecting more people to the Hippocratic Oath.[23] Technology, while drastically improving the quality of medical care since the time of Hippocrates, has only complicated the physician-patient dynamic further. As such, some medical professionals have called for the revision of the Hippocratic Oath with the rise of Big Data.[24] These professionals seek to amend the Oath by (1) including language that addresses the data obtained by both researchers and patients themselves since data is no longer collected by just physicians, (2) the specific acknowledgement of preventative health care rather than just "sick care," (3) the digital technology, such as algorithms, used for diagnoses, and (4) the explicit statement that doctors will aim to protect patient *data*.[25]

---

[20] *Id.*
[21] *Id.* at 7-8.
[22] *Id.* at 8.
[23] *Id.*
[24] *See generally* Bertalan Meskó & Brennan Spiegel, *A Revised Hippocratic Oath for the Era of Digital Health*, 24(9) J. MED. INTERNET RSCH. 1, 2 (2022).
[25] *Id.* at 2-3.

It is important to note that the developers of mHealth apps are not expected to partake in the Hippocratic Oath as they are not doctors. Therefore, these proposed revisions still will not correct the growing concern of mHealth apps. Some advocate for a "digital Hippocratic Oath" which would force "digital health innovators to embrace regulation" that "hold[s] apps up to a standard of conduct."[26] However, it may be more beneficial to enact strict privacy legislation that imposes fines for misconduct to truly ensure that app developers are exercising the utmost care with their customers' health data.

### *B. Personalized Medicine and the Mystery of Black-Box Treatment Plans*

Another aspect that has revolutionized modern healthcare is the concept of personalized medicine. Personalized medicine can be characterized as the nexus between Big Data and Big Health; this form of healthcare incorporates personal information derived from various types of medical tests, and other relevant data points, to create treatment plans tailored to individual patients.[27] The benefits to personalized health are immeasurable. By individualizing medicine, health practitioners can create "more precise marker-assisted diagnos[es,]" as well as "safer and more effective treatment[s],"[28] for patients while simultaneously "lower[ing] costs and improv[ing] the efficiency of the healthcare system."[29] This phenomenon enables "pharmaceutical and biotechnology industries [to] focus drug development efforts on

---

[26] Laura Lovett, *Aneesh Chopra Urges Innovators to Embrace 'Digital Hippocratic Oath'*, HEALTHCARE IT NEWS (Apr. 2, 2018, 9:45 AM), https://www.healthcareitnews.com/news/aneesh-chopra-urges-innovators-embrace-digital-hippocratic-oath.

[27] W. Nicholson Price II, *Black-Box Medicine*, 28 HARV. J.L. & TECH. 419, 420 (2015); *see also* Isaac S. Chan & Geoffrey S. Ginsburg, *Personalized Medicine: Progress and Promise*, 12 ANN. REV. GENOMICS & HUM. GENETICS 217 (2011) (explaining that personalized medicine takes into account family health history, health risk assessments, genomic information, including genome-wide variation, transcriptomics (the "genome-wide study of RNA expression levels in a cell, tissue or biological fluid"), metabolomics (the analysis of "changes in the nonprotein small molecules related to a biological or physiological state" through the use of mass spectroscopy and nuclear magnetic resonance spectroscopy), epigenomics ("the genetic programing that occurs predominantly as a consequence of DNA methylation (194)"), and, lastly, proteomics (the "large scale study of proteins"), to determine susceptibility to diseases, cancer, and more).

[28] Geoffrey S. Ginsburg & Jeanette J. McCarthy, *Personalized Medicine: Revolutionizing Drug Discovery and Patient Care*, 19 TRENDS BIOTECHNOLOGY 491, 495 (2001).

[29] Price II, *supra* note 27, at 427.

subpopulations who have the same critical genetic variants,"[30] thereby creating benefits for not only the sole patient being treated but thousands of genetically-similar individuals.

Personalized medicine can be divided into two categories: "[e]xplicit personalized medicine" and "black-box medicine."[31] Explicit personalized medicine uses scientific data and clinical research to analyze biological relationships to hypothesize the potential outcomes of medical treatments for individual patients.[32] This first category of personalized medicine is explicit because the data points and clinical research that was used in determining a treatment plan allows practitioners to understand why a patient is being treated in a particular way. Where major concern lies, however, is what W. Nicholson Price II labels as black-box medicine.

Black-box medicine can be defined as a system in which "opaque computational algorithms" are used to create a personalized medical plan "based on relationships which are *not* understood and often not identified."[33] This implicit personalized medicine regime utilizes large and broad data sets to make predications and treatment plans "without explicitly identifying or understanding those connections."[34] By uploading health information about a patient, or even family medical history, computers now have the ability to create a treatment plan that can be sent directly to a patient. This new ability is in sharp contrast from having a doctor explain a treatment method face-to-face with a patient explaining why the patient should be treated in a particular way. However, computers are unable to complete this task unless they have access a concerningly large amount of health information from all over the world.

An additional concern is the actual opacity of black-box medicine. Patients, including users of mHealth apps, do not understand how the algorithms work or how the algorithms create their final findings. So, not only do patients and app users not understand how the treatment is created, but these individuals do not know which data points are being used to make health-related analyses. It begs the question: how much information are these computers using and are users giving the computers more information than necessary?[35]

---

[30] *Id.*
[31] *Id.* at 425.
[32] *Id.* at 427.
[33] *Id.* at 425.
[34] *Id.* at 429-30.
[35] A potential concern is that this uneasiness about black-box medicine may inevitably evolve into concerns about algorithmic contracts. As the world increasingly becomes

The final line of defense for these concerns is privacy law, specifically in relation to mHealth apps. If mHealth apps are not subjected to the Hippocratic Oath, and the computers generating health treatments are utilizing health data points in a way unbeknownst to both medical professionals and those being treated, there must be a way to vigilantly protect the sensitive medical information of those in need of healthcare treatments. This problem has only been exacerbated after the Covid-19 pandemic as telehealth and mHealth treatments have become more accessible and utilized.[36] The United States must review its existing policies surrounding the protection of digital health information. Additionally, it will be beneficial to analyze and compare how other regions of the world are approaching this issue as well. Specifically, the United Sates should look to the European Union (EU) and their use of the General Data Protection Regulation (GDPR) as a potential example of how to enact all-encompassing privacy regulations, as the GDPR has been regarded as successful in forcing companies in becoming more aware and cautious when handling consumer data.[37]

## III. U.S. APPROACH TO PRIVACY FOR MHEALTH DATA PROTECTION

Currently, the United States does not have nationwide data privacy legislation.[38] Rather, "the federal regulations [concerning mHealth privacy] are so piecemeal that nearly every state has enacted its

---

digitalized, and black-box medicine becomes more institutionalized due to its efficient nature, computers will begin to determine what information they need and do not need. This in turn may affect the terms of contracts. Since doctors will rely on algorithms to determine treatment plans, it is foreseeable that the medical and digital health fields will come to rely on algorithms for contract formation. These algorithmic contracts, similar to that of black-box medicine, are "not analyzable simply as the sum of their inputs" as they are derived from complex variables that are inputted into computational relationships. Lauren Henry Scholz, *Algorithmic Contracts*, 20 STAN. TECH. L. REV. 128, 135 (2017). While there are mutual assent concerns over black-box algorithmic contracts, thereby making them likely unenforceable, it is imperative to keep these potential algorithmic contractual concerns in the background of a privacy analysis so that computers do not enable the release of private health information to potential third parties or collect more information than what is needed to determine a treatment plan.

[36] *See generally* Tsion H. Tebeje & Jorn Klein, *Applications of e-Health to Support Person-Centered Health Care at the Time of COVID-19 Pandemic*, 27 TELEMEDICINE & E-HEALTH 150 (2021). *See also* Bokolo Anthony Jnr, *Implications of Telehealth and Digital Care Solutions During COVID-19 Pandemic: A Qualitative Literature Review*, 46 INFORMATICS FOR HEALTH & SOC. CARE 68, 68 (2021).

[37] Ilse Heine, *3 Years Later: An Analysis of GDPR Enforcement*, CTR. FOR STRATEGIC & INT'L STU. (Sept. 13, 2021), https://www.csis.org/blogs/strategic-technologies-blog/3-years-later-analysis-gdpr-enforcement.

[38] Shaun G. Jamison, *Creating a National Data Privacy Law for the United States*, 10 CYBARIS, AN INTELL. PROP. L. REV. 1, 3 (2019).

own regulations to provide additional privacy protections for personal data, health information, and genetic information."[39] The United States, as a whole, presently relies on the Health Insurance Portability and Accountability Act (HIPAA), the Federal Trade Commission (FTC), and the Food & Drug Administration (FDA) when navigating privacy and health data.[40]

### *A. HIPAA: The Privacy Rule & the Security Rule*

In 1996, HIPPA was passed to "to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes."[41] It is currently the main federal statute that relates to mHealth, especially after the Standards for Privacy of Individually Identifiable Health Information (the Privacy Rule) was passed.[42] According to the U.S. Department of Health & Human Services (HSS), the Privacy Rule "establishes national standards to protect individuals' medical records and other individually identifiable health information," also known as personal health information, and "applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically."[43] Personal health information (PHI) is any

---

[39] Marilyn Cech, *Genetic Privacy in the "Big Biology" Era: The "Autonomous" Human Subject*, 70 HASTINGS L.J. 851, 867-68 (2019).

[40] The FDA has a very limited view of what constitutes a medical device (e.g., mHealth apps). Since the software of some of these mHealth applications do not fall under the definition of "device" in the Federal Food, Drug, and Cosmetic Act (FD&C Act), the FDA will refrain from regulating them as devices. For the mHealth applications that could function as medical devices but pose a low risk to the public, the FDA will most likely exercise enforcement discretion over them rather than enforce the FD&C Act. U.S. FOOD & DRUG ADMIN., Policy for Device Software Functions and Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff, 1, 2 (Sept. 28, 2022), https://www.fda.gov/media/80958/download; Federal Food, Drug, and Cosmetic Act, 21 U.S.C. §§ 301-399i (2021).

[41] Preamble, Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

[42] Helm & Georgatos, *supra* note 1, at 152.

[43] *The HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS. (Mar. 31, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/index.html ("The Rule requires appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of such information without an individual's authorization. The Rule also gives individuals rights over their protected health information, including rights to examine and obtain a copy of their health records, to direct a covered entity to transmit to a third party an

information that relates to someone's previous or current health conditions, the healthcare treatment someone is receiving, or any payment in regards to health procedures both in the past or present; essentially, PHI is defined as any sensitive health information by which an individual could be identified.[44] HIPAA further protects PHI through the Security Standards for the Protection of Electronic Protected Health Information (the Security Rule). The Security Rule specifically protects PHI that is "held or transferred in electronic form" (e-PHI).[45] The creation of both the Privacy Rule and the Security Rule was a response by the HSS to the growing concern of the healthcare industry becoming reliant on technology to complete basic functions.[46] These rules were seen as compromises that enable healthcare providers to continue using new technologies that make their profession more efficient, while simultaneously protecting the health information of patients.[47] With this being said, there are important limitations to HIPAA in regard to mHealth.

There are two specific concerns with HIPAA's Privacy and Security rules. First, these rules only apply to "covered entities."[48] According to HSS, covered entities refer to "health plans, health care clearinghouses, and [] any health care provider who transmits health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA."[49] mHealth app developers are not specifically listed, therefore, they may not be subjected to HIPAA standards. Second, the Privacy and Security Rules refer to e-PHI that is identifiable; e-PHI that has been made to be anonymous or in the public domain do not apply to the rules.[50] While it could be argued that deidentified information can protect users, this claim is not necessarily true.

First, it is false to proclaim that just because health information has been wiped from identifiers that the information cannot be traced back to the individual from which the information is derived, as scientists

---

electronic copy of their protected health information in an electronic health record, and to request corrections.").

[44] *Summary of the HIPAA Privacy Rule,* U.S. DEP'T OF HEALTH & HUM. SERVS (Oct. 19, 2022), https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

[45] *Id.*

[46] *Id.*

[47] *Id.*

[48] Cech, *supra* note 39, at 869.

[49] *Summary of the HIPAA Privacy Rule*, *supra* note 44.

[50] Cech, *supra* note 39, at 869.

have proven this time and time again.[51] Second, covered entities are able to disclose this "deidentified" information,[52] which in turn creates a multi-billion dollar marketplace where third-party buyers and sellers trade health information, even though one could potentially still identify someone with this information.[53] Third, insurance companies have the ability to discriminate based on deidentified information that was collected from the public domain.[54] Thus, these concerns regarding covered entities and the handling of deidentified information can be combined into the troubling conclusion that "HIPAA governs what covered entities do, not what becomes of personal information once it leaves the covered entities' control."[55] It is also important to note that an additional limitation of HIPAA is that it only addresses the e-PHI that alludes to treatment and not the surplus information that mHealth apps can gather that does not necessarily pertain to the health treatment that one is seeking, such as geo-location, usage, and more. Therefore, while HIPAA offers some protection with respect to an individual's e-PHI, it is sorely inadequate when put into context with mHealth apps.

### *B. FTC & mHealth*

The Federal Trade Commission (FTC)'s mission is to "[protect] the public from deceptive or unfair business practices and from unfair

---

[51] Melissa Gymerk et al., *Identifying Personal Genomes by Surname Inference*, 339 SCI. 321, 324 (2013) (detailing how the use of a free and publicly accessible Internet resources, as well as the use of a surname inference, led to the identification of nearly 50 individuals whose information was supposed to be anonymous on genetic genealogy databases); Luc Rocher et al., *Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models*, 10 NATURE COMMC'NS. 1, 5 (2019) (demonstrating how 99.98% of the people in Massachusetts can be re-identified by using 15 demographic attributes from "deidentified" datasets); *see* Katharine Miller, *De-Identifying Medical Patient Data Doesn't Protect Our Privacy*, STAN. UNIV. HUMAN-CENTERED A.I. (Jul. 19, 2021), https://hai.stanford.edu/news/de-identifying-medical-patient-data-doesnt-protect-our-privacy (". . . [I]t is never possible to guarantee that de-identified data can't or won't be re-identified. That's because de-identification is not anonymization. . . . In addition, since HIPAA was passed in 1996, artificial intelligence has only gotten better at identifying people using facial recognition, genetic information, iris scans, and even gait.").

[52] Cech, *supra* note 39, at 869.

[53] Christina Farr, *Hospital Execs Say They Are Getting Flooded with Requests for Your Health Data*, CNBC (Dec. 18, 2019, 8:27 AM), https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html.

[54] Cech, *supra* note 39, at 869; *see also* Marshall Allen, *Health Insurers Are Vacuuming Up Details About You—And It Could Raise Your Rates*, PROPUBLICA (Jul. 17, 2018, 5:00 AM), https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates.

[55] Fox, *supra* note 1, at 214.

methods of competition through law enforcement, advocacy, research, and education."[56] Anti-competitive concerns stem from "platform dynamics (e.g., Apple, Google, etc.) and how a powerful few corporations might hold consumers captive, monopolize the entirety of a mobile device user's experience, control consumer access to apps or data they generate, limit the rate of innovation or app options by dictating app features, and more."[57] Privacy concerns, such as lax data security and privacy measures, can also be calculated when determining if an entity is acting unfairly.[58] While some have argued that mHealth privacy concerns should be governed by more specific statues, like HIPAA or the Health Information Technology for Economic and Clinical Health Act (HITECH), the FTC has stated that the commission has "concurrent and complementary jurisdiction" in health privacy cases.[59] Therefore, the FTC has ability to rule on mHealth apps that have inadequate security features.[60]

The FTC also provides guides where mHealth app developers can determine which federal laws and regulations their app may be subjected to.[61] These guides provide information about HIPAA, the Federal Food, Drug, and Cosmetic Act (FD&C Act),[62] the 21st Century Cures Act,[63] the HHS Office of the National Coordinator for Health Information Technology (ONC)'s "information blocking" regulations,[64] the FTC's Health Breach Notification Rule,[65] and the Children's Online Privacy

---

[56] FED. TRADE COMM'N, ABOUT THE FTC, https://www.ftc.gov/about-ftc (last visited April 18, 2023).
[57] Jennifer K. Wagner, *The Federal Trade Commission and Consumer Protections for Mobile Heath Apps*, 48 J. L. MED. & ETHICS 103, 105 (2020).
[58] *Id.*
[59] Helm & Georgatos, *supra* note 1, at 163 (citing Respondent LabMD, Inc.'s Motion to Dismiss the Complaint with Prejudice and Stay Administrative Proceedings at 9, *In the Matter of LabMD, Inc.,* No. 9357, F.T.C. (Aug. 28, 2013)).
[60] *Id.*
[61] Mobile Health App Interactive Tool, FED. TRADE COMM'N, (Dec. 2022) https://www.ftc.gov/business-guidance/resources/mobile-health-apps-interactive-tool.
[62] *Id.* ("When a software function is intended for use in the diagnosis of disease or other conditions, or the cure, mitigation, treatment, or prevention of disease, or is intended to affect the structure or any function of the human body, the software function is a device under section 201(h) of the FD&C Act, if it is not a software function excluded from the device definition by the 21st Century Cures Act.").
[63] 21st Century Cures Act, Pub. L. No. 114-255, 130 Stat. 1033 (2016).
[64] Information blocking is a practice that "is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information" by either health care providers, health IT developers, or by a health information network. *Id.* at § 4004, 130 Stat. 1176.
[65] The Health Breach Notification Rule requires "entities covered by the Rule to provide notifications to consumers, the FTC, and, in some cases, the media, following certain breaches of personal health record information," and applies to other mHealth

Protection Act (COPPA).[66] It is important to note, however, that use of these guides is not required by law, thus it is up to the developer's discretion of whether or not to utilize the tools provided by the FTC.[67]

Major concerns with the FTC's regulations of privacy issues in mHealth apps lie in its reliance on laws that use broad standards for issues like consumer protection.[68] As technology becomes more advanced and nuanced, there is the possibility that broad rules such as the ones used by the FTC will become outdated, thereby challenging the FTC's authority on privacy issues.[69] Additionally, some have argued that FTC's inability to immediately fine an offending organization makes the FTC a poor deterrent mechanism for privacy concerns.[70]

### *C. State Privacy Laws*

Since there is a lack of a nationally recognized and comprehensive data privacy law in the United States, the states themselves are free to create privacy regulation on their own terms. Often, these State regulations vary depending on region or the types of data that they apply to.[71] Notable states that have created comprehensive consumer data privacy laws are California,[72] Colorado,[73] Connecticut,[74] Utah,[75] and

---

apps as they act as quasi-healthcare providers by "furnishing health services or supplies" to consumers. Mobile Health App Interactive Tool, *supra* note 61.

[66] COPPA gives parents the ability to oversee the collection of personal information from their children. It specifically applies to any internet source that is aimed at children under thirteen, and the operator of such source has access to the personal information of a child, including photos, videos, geolocation, and more. Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6505 (1998).

[67] Mobile Health App Interactive Tool, *supra* note 61.

[68] Helm & Georgatos, *supra* note 1, at 163.

[69] *Id.*

[70] Jamison, *supra* note 38, at 8.

[71] Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, N.Y. TIMES (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/. Please note that this piece was written before the enactment of the My Health My Data Act in Washington State. This broad Act aims to increase the obligations of non-HIPAA covered entities that handle sensitive consumer health data. Future analysis is required to see the effects and reliability of this Act as most of the Act's provisions will come into effect in 2024. Yana Komsitsky & Neeka Hodaie, *Washington's "My Health My Data" Act*, SEYFARTH SHAW LLP (Apr. 25, 2023), https://www.seyfarth.com/news-insights/washingtons-my-health-my-data-act.html.

[72] California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100-1798.199.100 (West 2018). [hereinafter CCPA].

[73] Colorado Privacy Act, COLO. REV. STAT. §§6-1-1301-6-1-1313 (2021).

[74] An Act Concerning Personal Data Privacy and Online Monitoring, CONN. GEN. STAT. § 22-15 (2022) (effective July 1, 2023).

[75] Utah Consumer Privacy Act, UTAH CODE ANN. §§13-61-101-13-61-404 (West 2022) (effective Dec. 31, 2023).

Virginia.[76] As California's legislation has been enacted the longest, it is the most useful tool to analyze state privacy regulation with respect to mHealth.

The California Consumer Protection Act (CCPA) is the closest U.S. act to resemble the rules and regulations of the GDPR.[77] It specifically concerns itself with protection of the personal information of the residents of California and defines personal information as any "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*."[78] The CCPA focuses on granting five essential rights with respect to data privacy in California; according to the Act, Californians are entitled to i) know what information about them are being collected, ii) know if their information is being bought, sold, or disclosed to other individuals, iii) refuse data collection or processing, iv) access their own personal data, and, lastly, v) be free from discrimination if they were to exercise one of their privacy rights.[79] Violations regarding the processing of personal information or preventing an individual from invoking their privacy rights may result in fines, thus major multinational corporations have changed their behaviors to be in accordance with the CCPA.[80] For health data specifically, the CCPA requires that companies provide an opportunity for consumers to opt out of the sale of their data.[81] Lastly, an additional Californian privacy act, the California Privacy Rights Act (CPRA), works tangentially with the CCPA to mandate data impact assessments for companies handling personal information, as well as mandate the minimization of the collection of one's personal data as much as possible.[82]

There has recently been a focus on the privacy issues concerning mobile applications in California. Californian Attorney General Rob

---

[76] Consumer Data Protection Act, VA. CODE ANN. §§ 59.1-575-59.1-585 (2023).
[77] Cech, *supra* note 39, at 884.
[78] CCPA, *supra* note 72, at § 1798.140(v)(1) (emphasis added). This Californian definition of "personal information" provides a broader category than what is actually afforded under the GDPR, as explained in Part IV, as it also includes information about consumer households. Cech, *supra* note 39, at 884.
[79] Cech, *supra* note 39, at 884.
[80] Hannah K. Galvin & Paul R. DeMuro, *Developments in Privacy and Data Ownership in Mobile Health Technologies, 2016-2019*, 29(1) Y.B. MED. INFORMATICS 32, 34 (2020).
[81] Danielle Feingold, *Digital Health Companies and Data Protection: Ensuring Compliance with Continually Evolving, Piecemeal State Regulations Surrounding Data Use and Data Subject Rights*, 31 ANNALS HEALTH L. ADVANCE DIRECTIVE 147, 158-59 (2021).
[82] *Id.* at 157.

Bonta conducted an investigation regarding the privacy policies of certain mobile apps, and the investigation resulted in a wide range of companies from various sectors being notified that their mobile applications failed to comply with the CCPA.[83] The sweep focused on failed consumer opt-out requests, the lack of a mechanism to stop the sale of data, failed processing of consumer requests, and more.[84] When speaking about the importance of privacy regulation for mobile apps, Attorney General Bonta stated,

> [Every day] businesses must honor Californians' right to opt out and delete personal information, including when those requests are made through an authorized agent[,] particularly given the wide array of sensitive information that these apps can access from our phones and other mobile devices. I urge the tech industry to innovate for good — including developing and adopting user-enabled global privacy controls for mobile operating systems that allow consumers to stop apps from selling their data.[85]

## IV. EU AND THE GDPR

Enacted on May 25th, 2018, the GDPR was created as a means to promote uniformity and harmonization of data protection and privacy laws within the European Union.[86] According to Article 4 of the GDPR, "personal data" is any identifiable information relating to a person, such as a name, identification number, or any factor that relates specifically to a person's physical, physiological, genetic, mental, economic, cultural or social identity."[87] Health data occupies a specific subset of the GDPR's personal data as it is categorized as "sensitive data." Sensitive data encompasses information that refers to an individual's genetic data, biometric data, "racial or ethnic origin, political opinions, religious or

---

[83] *Ahead of Data Privacy Day, Attorney General Bonta Focuses on Mobile Applications' Compliance with the California Consumer Privacy Act*, STATE CALI. DEP'T JUST. (Jan. 27, 2023), https://oag.ca.gov/news/press-releases/ahead-data-privacy-day-attorney-general-bonta-focuses-mobile-applications'.
[84] *Id.*
[85] *Id.*
[86] Council Regulation 2016/679, Regulation on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, 2016 O.J. (L. 119) 1 [hereinafter GDPR].
[87] Achilleas Papageorgiou et al., *Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice*, 6 INST. ELEC. AND ELECS. ENG'R ACCESS 9390, 9400 (2018).

philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."[88] The GDPR mandates that companies handling any sort of sensitive data act responsibly so that consumers have the ability to access and understand what data is being collected from them, why the data is being processed, and who is collecting such information.[89] Consequently, the definitions for personal data and health data are intentionally broad so that the GDPR is applicable to not only to companies producing medical devices, but also to the developers of commercial apps for wearable-medical devices, such as a fitness watch, that could potentially handle sensitive data.[90]

A notable aspect of the GDPR is that the regulation has established certain rights that individuals are entitled to when their personal data is being handled. Examples of these rights include: (1) an explanation as to why their data is being used; (2) the requirement of affirmative consent to process personal data; (3) withdrawal of consent to use personal data; (4) the ability to access personal data in a "readable and accessible format;" (5) the erasure of personal data ("a right to be forgotten"); and (6) the ability to transfer data to another provider ("right of portability").[91] The GDPR also mandates that entities obtain consent before any data is handled,[92] and provide "at least one of the six legal bases for processing data."[93] Failure to comply with the GDPR standards will result in high fines.[94] Additionally, companies must provide data impact assessments to regulators if they are to process data that would "present a high risk to the rights of [the] persons" from whom they are collecting data from.[95] Lastly, the GDPR mandates that data controllers exercise a principle called "data minimization," where essentially collectors limit the amount of information that they gather from an

---

[88] *Id.* at 9401.
[89] T. Mulder & M. Tudorica, *Privacy Policies, Cross-Border Health Data and the GDPR,* 28(3) INFO. & COMMC'NS. TECH. L. 261, 262 (2019).
[90] *Id.* at 264.
[91] Feingold, *supra* note 81, at 153; *see generally* GDPR, *supra* note 86.
[92] According to Article 4 of the GDPR, consent is "any freely given, specific, informed and unambiguous indication of a data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her." GDPR, *supra* note 86, at art. 4(11).
[93] Feingold, *supra* note 81, at 153.
[94] *See* GDPR, *supra* note 86, at art. 83.
[95] Feingold, *supra* note 81, at 153-54 (citing Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 DENV. L. REV. 93, 118 (2020)) ("The data auditing and related impact assessment requirements ensure the adequate involvement of citizens in managing their data and promote corporate accountability of data processing.").

individual to only the amount necessary to complete their specified task.[96]

Not only does the GDPR place a great emphasis on consent, but there are other conditions that the GDPR forces companies to comply with that are of great importance. One of these conditions is the use of clear and plain language.[97] The second condition is transparency, which is crucial as a person needs to know who is handling their data, as well as what their risks, rules, safeguards and rights are.[98] Lastly, the final component of the GDPR that is of extreme importance is the ease by which an individual can protect their sensitive health data when it crosses borders.[99] Health data is in constant flux; the transfer of data can simply be from a wearable device to an online server, or on a much broader scale, such as the uploading of sensitive information in one country to the database of a company located in a different country. As stated by some privacy scholars, "[o]ne of the consequences of the electronic capturing of personal data via modern technologies is that, due to the very nature of these modern technologies, data may be located and stored anywhere in the world."[100] Understandably, the creators of the GDPR were worried about not only the transfer of data between EU countries, but also the transfer of data about EU citizens to countries located outside of the EU. As such, the GDPR mandates that non-EU companies must still comply with the GDPR's sensitive data regulations when handling the data of subjects within the EU.[101]

While the GDPR establishes EU standards of how to treat health data, member states are still able to adopt state-specific privacy legislation so long as it is compatible with the GDPR regulations.[102] As

---

[96] GDPR, *supra* note 86, at art. 5(1)(c).
[97] *Id.* at art. 7(2).
[98] Mulder & Tudorica, *supra* note 89, at 268. An added component to the transparency aspect of the GDPR is that companies must also make individuals aware that they can exercise their rights when it pertains to the protection and use of their personal data. *Id.* at 269.
[99] *Id.* at 271.
[100] *Id.*
[101] *Id.* at 272.
[102] *See, e.g.*, Fruzsina Molnár-Gábor et al., *Harmonization after the GDPR? Divergences in the Rules for Genetic and Health Data Sharing in Four Member States and Ways to Overcome Them by EU Measures: Insights from Germany, Greece, Latvia and Sweden*, 84 SEMINARS CANCER BIOLOGY 271, 272-73 (2022) (comparing the health data protection laws of different EU countries, such as Germany's Federal Data Protection Act (BDSG), Greece's Greek Data Protection Act (DPA), Lativa's Personal Data Processing Law (PDPL), and both of Sweden's Patient Data Act (PDA) and Swedish Ethical Review Act (ERA)).

such, there are some wide variances between how health data is handled by EU countries.[103] Some of which are detailed below.

### *A. A Conservative Approach: Germany*

The German Federal Data Protection Law (BDSG) and the Bundestag Data Protection Adaptation and Implementation Act EU (DSAnpUG-EU) are the official German legal adaptations of the GDPR.[104] Like the GDPR, the BDSG places health data under a special category of personal data, and only enables the processing of this data when it is "strictly necessary for the performance of the controller's task."[105] The BDSG mandates that certain safeguards are implemented when handling special personal data, like health data. Examples of such safeguards include: (1) the identification of specific requirements for data security/protection; (2) time limits for the amount of time it takes to determine relevance and subsequent erasure; (3) easy determination of who is handling special data; (4) restriction of who can handle special data; (5) separation of processing special data from other types of personal data; (6) deidentification of special data; (7) encryption of special data; or the (8) implementation of specific standards to make certain that special data is being handled lawfully.[106] Additionally, the BDSG also delineates the rights of data subjects with respect to data processing,[107] requirements for the security of data processing,[108] notification procedures for a personal data breach,[109] rules for conducting a data protection impact assessment,[110] and much more. Lastly, the BDSG imposes strict rules for consent, such as having "explicit" consent for special personal data.[111] Such safeguards and

---

[103] Marieke Bak et al., *You Can't Have AI Both Ways: Balancing Health Data Privacy and Access Fairly*, 13 FRONTIERS IN GENETICS 1, 2 (2022).
[104] Fruzsina Molnár-Gábor, *Germany: A Fair Balance Between Scientific Freedom and Data Subjects' Rights?*, 137 HUMAN GENETICS 619, 619 (2018).
[105] Bundesdatenschutzgesetz (BDSG) "Federal Data Protection Act of 30 June 2017" (Federal Law Gazette I p. 2097), as last amended by Article 10 of the Act of 23 June 2021 (Federal Law Gazette I, p. 1858; 2022 I p. 1045) (Ger.), https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.pdf ("'[D]ata concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.").
[106] *Id.* at pt 3, ch. 2 §48.
[107] *Id.* at pt 3, ch. 2 §55.
[108] *Id.* at pt 3, ch. 2 §64.
[109] *Id.* at pt 3, ch. 2 §§65; 66.
[110] *Id.* at pt 3, ch. 2 §67.
[111] *Id.* at pt 3, ch. 2 §51.

procedures are one of many ways in which Germany exceeds the minimum set of protections enforced by the GDPR.[112] Note that depending on the health service that a mHealth app provides, there may be more regulations that the developer can be subject to, and failure to comply with these regulations may result in sanctions or fines up to EUR 20 million.[113]

Implemented on June 27th, 2019, the DSAnpUG-EU was intended to reconcile the nearly 154 federal laws from the BDSG with the changes to the GDPR over the previous few years.[114] Major changes to the BDSG include the increased minimum number of employees, from ten to twenty, who are hired to processes personal data, and simplified consent requirements from employees within the scope of their employment.[115] The DSAnpUG-EU also includes the addition of another provision of permission when processing special health data; according to the new law, non-public bodies may be able to process special data only when it is "absolutely necessary for reasons of substantial public interest."[116]

### *B. A Liberal Approach: Finland*

With respect to mHealth apps, the Data Protection Act of Finland (DPA) and the Act on the Secondary Use of Health and Social Data (ASUHSD) are the most useful to analyze for data protection for health

---

[112] Anna Essén et al., *Health App Policy: International Comparison of Nine Countries' Approaches*, 31 NPJ DIGIT. MED. 1, 6 (2022); *see also* David Raj Nijhawan*, The Emperor Has No Clothes: A Critique of Applying the European Union Approach to Privacy Regulation in the United States*, 56 VAND. L. REV. 939 (2003) (explaining the Germany, much like France, have stricter laws than other EU-member states). *But see The New German Privacy Act*, Deloitte, https://www2.deloitte.com/dl/en/pages/legal/articles/neues-bundesdatenschutzgesetz.html (last visited Jan. 31,2023, 6:48 AM) (explaining that differing German and EU laws cause uncertainty for data controllers and processors, and that the GDPR is the superior rule of law, thus causing national laws to only be generated when the GDPR provides opening clauses).

[113] Jana Grieb et al., *Digital Health Laws and Regulations Germany*, ICLG (Feb. 24, 2022), https://iclg.com/practice-areas/digital-health-laws-and-regulations/germany#.

[114] Detlev Gabel, *German Bundestag Passes Second Act on the Adaptation of Data Protection Law to the GDPR*, WHITE & CASE (Jul. 19, 2019), https://www.whitecase.com/insight-alert/german-bundestag-passes-second-act-adaptation-data-protection-law-gdpr.

[115] *Id.*

[116] Lars Lensdorf, *German Bundestag Approves 2nd German Data Protection Adaptation Act ("2nd DSAnpUG"): Summary of Significant Changes for German Data Protection Laws*, COVINGTON: INSIDE PRIVACY (Jul. 3, 2019), https://www.insideprivacy.com/eu-data-protection/german-bundestag-approves-2nd-german-data-protection-adaptation-act-2nd-dsanpug-summary-of-significant-changes-for-german-data-protection-laws/.

information. [117] The DPA, like the BDSG, supplements the EU's GDPR. However, unlike its German counterpart, the DPA does not explicitly describe personal data protection.[118] In fact, the main intention of the DPA is to "reduce special regulation" so that Finland is more reliant on the general articles of the GDPR.[119] When necessary, Finland uses sector-specific regulations to deal with particular subsets of data protection, such as the ASUHSD.

The ASUHSD was created to "facilitate the effective and safe processing and access to the personal social and health data for steering, supervision, research, statistics and development in the health and social sector."[120] Secondary use is when the data collected from an individual, in this instance health data, is used for a reason other than the primary justification for the collection of the data.[121] What is unique about this Act is that it creates an "established IT ecosystem," known as Findata,[122] that facilitates the transfer of social and health care information from data controllers that were responsible for the primary purpose of processing to other public or private entities that obtain a fixed-term revocable license.[123] Findata differs from other EU member states' centralized data

---

[117] Tietosuojalaki [Data Protection Act] (Finlex 1050/2018) (Fin.), https://www.finlex.fi/en/laki/kaannokset/2018/en20181050.pdf; Laki Sosiaali- Ja Terveystietojen Toissijaisesta Käytöstä [Act on Secondary Use of Social and Health Data](Finlex, 552/2019), https://stm.fi/documents/1271139/1365571/The+Act+on+the+Secondary+Use+of+Health+and+Social+Data/a2bca08c-d067-3e54-45d1-18096de0ed76/The+Act+on+the+Secondary+Use+of+Health+and+Social+Data.pdf.

[118] Päivi Korpisaari, *Finland: A Brief Overview of the GDPR Implementation*, 5 EUR. DATA PROT. L. REV. 232, 232 (2019).

[119] *Id.* at 233. Germany's BDSG can be seen to do the opposite; the BDSG can be construed as a mechanism that is seeks to impose extra restrictions than what the GDPR stipulates. *GDPR in Germany: What You Need to Know in 2022*, PANDECTES (Jan. 2, 2022), https://pandectes.io/blog/gdpr-in-germany-what-you-need-to-know-in-2022/.

[120] *Secondary Use of Health and Social Data*, MINISTRY OF SOCIAL AFFAIRS AND HEALTH, https://stm.fi/en/secondary-use-of-health-and-social-data (last visited Jan. 31, 2023).

[121] *Id.* The types of secondary uses that are authorized through the ASUHSD are "scientific research, statistics, development and innovation operations, steering and supervision by authorities, planning and reporting duty of an authority, education and knowledge management." *Act on the Secondary Use of Health and Social Data*, UNIV. E. FIN. LIBR., https://www.uef.fi/en/library/act-on-the-secondary-use-of-health-and-social-data (last visited Feb. 1, 2023).

[122] *See generally Services for Customers*, FINDATA, https://findata.fi/en/services-for-customers/ (last visited Feb. 1, 2023).

[123] Joonas Dammert, *Finland: Parliament Approves New Act on the Secondary Use of Social and Health Care Personal Data*, DLA PIPER (Apr. 8, 2019), https://blogs.dlapiper.com/privacymatters/finland-parliament-approves-new-act-on-the-secondary-use-of-social-and-health-care-personal-data/; *see also GA4GH GDPR Brief: The Finnish Secondary Use Act 2019 (May 2020 Bonus Brief)*, GLOB. ALL. FOR

systems by how it labels accessible data. Findata labels accessible data in numerous ways. The labels can be generated by either using a patient's full name, a patient's national civic number/patient ID, an algorithmic pseudonym of the patient's name, an algorithmic pseudonym of the patient's ID number, a pseudonym from other factors, or by using completely anonymized data.[124]

Finland, like other EU member states, continues to prioritize data subjects' consent with the ASUHSD. First, explicit consent is needed for any secondary use pertaining to innovation or development activities.[125] Second, data users have the ability to contact the employees of Findata to either alter or withdraw their secondary use consent.[126] Third, the data subject must consent to both Findata *and* the secondary user; this can be done either simultaneously when the data subject consents to the primary data controller using their data, or by having the data user consent to the primary data controller first and expressing consent to Findata and the secondary user later on.[127] It is important to note that the above illustrations are specifically in relation to secondary use.[128] The Finnish stance towards secondary use can be construed as a liberal one; the ASUSHD is essentially "a national policy oriented towards big data and open data to transform the technical and governance infrastructure for AI and other computer science research."[129] Some EU countries, like Germany, do not currently have a nationally-recognized process for secondary use due to concerns about consent, the use of personal health data, and more.[130]

---

GENOMICS & HEALTH (May 21, 2020), https://www.ga4gh.org/news/ga4gh-gdpr-brief-the-finnish-secondary-use-act-2019-may-2020-bonus-brief/ (explaining the creation of Findata in 2020 to handle the requests for secondary use of social and health data).

[124] Eur. Comm'n, Consumers, Health, Agric. and Food Exec. Agency, Assessment of the EU Member States' Rules on Health Data in the Light of GDPR, No SC 2019 70 02 in the Context of the Single Framework Contract Chafea/2018/Health/03, at 111-12, (2021) https://health.ec.europa.eu/system/files/2021-02/ms_rules_health-data_en_0.pdf.

[125] Dammert, *supra* note 123.

[126] *Id.*

[127] *Id.*

[128] For example, "[i]n Finland, consent is not legally required for including personal data in national health registries." Bak, *supra* note 103, at 2.

[129] *Id.*

[130] *See generally* Sven Zenker et al.*, Data Protection-Compliant Broad Consent for Secondary Use of Health Care Data and Human Biosamples for (Bio)Medical Research: Towards a New German National Standard*, 131 J. BIOMEDICAL INFORMATICS 104096, 2-8 (2022).

## V. THE ULTIMATE CHOICE: EU'S GDPR PATH OR THE ROAD LESS TRAVELED

As Big Data becomes more pervasive in society's daily activities and functions, the United States is faced with the dilemma of finding the best approach to protect American citizens' data. Two of the major arguments within this debate is whether the United States should adopt a comprehensive data policy like the EU's GDPR, or if the United States should adopt an approach that is uniquely its own by allowing States to choose what data protection policies they want to enact for their residents. Therefore, it is necessary to weigh the pros and cons of the application of the GDPR approach to the American legal regime, especially with respect to health data and mHealth apps.

There are many beneficial aspects to adopting a comprehensive, national standard for data privacy in the United States. As not only healthcare but other daily functions become digitized, the United States will have to start concerning itself with multiple entities having access to people's sensitive data. Currently, the United States has adopted a data privacy approach that focuses on direct consumer relationships, thus making the policy vulnerable to unregulated third parties partaking in data processing.[131] In contrast, the EU's GDPR focuses on the personal data itself and not the entity that is controlling it, which in turn subjects even third parties to fall under the jurisdiction of the GDPR due to the sensitive nature of the data that they are handling.[132]

If the United States were to adopt a GDPR approach to privacy regulation, there are two benefits that could arise relating to third parties. First, the United States would not have to create additional legislation to account for third-party users, saving time and money for the legislative branch. Second, since many third-party companies are already changing their approach to data processing to accommodate the demands of the GDPR, creating legislation that mimics the GDPR could save money for multinational businesses, promote international business relations, and

---

[131] Jones & Kaminski, *supra* note 95, at 107; *see* Jill McKeon, *The Quest to Improve Security, Privacy of Third-Party Health Apps*, TECHTARGET: HEALTH IT SECURITY (Apr. 12, 2022), https://healthitsecurity.com/features/the-quest-to-improve-security-privacy-of-third-party-health-apps (noting that the "onus should not be on the individual" to find the most secure health app because they are the ones in need of finding healthcare, and that third-party privacy concerns expose the shortcomings of HIPAA).

[132] Jones & Kaminski, *supra* note 95, at 107.

provide clarity and foster transparency about third parties for data subjects and consumers.[133]

Another benefit derived from having federal legislation based on the GDPR is that rather than having too many drastically different state laws, there would be a minimum standard for privacy protection that all States would have to adhere to. Instead of relying on various acts and governmental organizations, like HIPPA, the FTC, or the FDA, the federal government can address all types of privacy concerns through one act. If States are still concerned about potential gaps in a federal act, they would have the ability to address those concerns in state-specific acts, similar to how EU-member states, like Germany and Finland, have their own privacy legislation. Having a national standard for privacy regulation will only reiterate the basic protections that Americans should be afforded with respect to their sensitive health data. It will also provide clarification about how American companies, and companies that operate in the United States, should treat and handle their consumers' data. Thus, mHealth app developers will understand American expectations of how to treat the data that they collect, especially regarding data sharing rights, opt-in consent, data minimization, and nondiscrimination for those who utilize their privacy rights.[134] Ultimately, a connection between the GDPR and U.S.-based privacy legislation will promote simplicity and standardization for companies and consumers all over the world.[135]

With all of this being said, the GDPR is not the perfect solution to the ever-growing list of privacy concerns. Some scholars have already determined that the GDPR, or any GDPR-like legislation, would be inadequate in solving the United States' privacy concerns.[136] There are three specific concerns about a GDPR-like federal privacy law in the U.S. The first is that a GDPR approach to privacy protection would interfere with American's First Amendment-protected right to the free flow of information.[137] Many companies rely on the easy transfer of information to successfully function; the GDPR, while well-intended, poses more obstacles in such movement. This creates concerns of having too much government involvement in the affairs of American citizens and

---

[133] Piotr Foitzik, *What You Must Know About 'Third Parties' Under GDPR and CCPA*, INT'L ASS'N PRIVACY PROS. (Nov. 26, 2019), https://iapp.org/news/a/what-you-must-know-about-third-parties-under-the-gdpr-ccpa/.
[134] Klosowski, *supra* note 71.
[135] *See generally* Foitzik, *supra* note 133.
[136] Nijhawan, *supra* note 112, at 944.
[137] *Id.* at 959.

companies,[138] the movement of lower quality information due to consumers' veto power against data collection,[139] and more. Essentially, the application of a GDPR approach to the U.S. would be "a problematic situation in the U.S., because the EU method of registering data processing activities does not align with American values of minimal government intrusion into the private sphere."[140]

The second concern is related specifically to digital health and, thus, mHealth apps. The GDPR has been criticized to be rooted in preconceived notions of data privacy, thereby making it incompatible with how digital health currently operates and how digital health will evolve.[141] For example, as seen with black-box medicine, healthcare providers have become reliant on the use of algorithms. As such, "personal health data collected for machine learning can be put to extensive uses that cannot be specifically identified and explicitly articulated to the data subject at the time of collection… as machine learning algorithms 'learn and develop' and hence are not necessarily directed by their programmers."[142] Therefore, digital health is already in contention with the GDPR data protection principles of data minimization and transparency. Another example of the GDPR's inadequacy with regard to mHealth apps is that the distinction between personal data and sensitive data can easily be blurred which undermines the protection enumerated in the EU legislation.[143] For instance, seemingly unrelated and unimportant data, like shopping records and lifestyle habits, could be linked to important information, such as an individual's health status; even if a mHealth app company were to treat both data sets differently, the company could still ultimately have the ability to create inferences about the innocuous data to create accurate assumptions about a consumer's sensitive information.[144]

Lastly, a critique about the American implementation of a GDPR-like legislation is that it will ultimately not influence American citizens anyway due to the "privacy paradox." The privacy paradox is when individuals, while valuing their right to privacy, ultimately make decisions that put their privacy at risk with respect to modern

---

[138] *Id.* at 961-62.
[139] *Id.* at 964.
[140] *Id.* at 967 (citing Paul Rose, Comment, *A Market Response to the European Union Directive on Privacy,* 4 UCLA J. INT'L L. & FOREIGN AFF. 445, 469-70 (1999/2000)).
[141] *See* Luca Marelli, Elisa Lievevrouw & Ine Van Hoyweghen, *Fit for Purpose? The GDPR and the Governance of European Digital Health*, 41 POL'Y STUD. 447, 452 (2020).
[142] *Id.* at 453.
[143] *Id.* at 455.
[144] *Id.*

technologies.[145] Examples of this phenomenon can be seen when consumers agree to a company's privacy policies without reading them, resulting in the consumer not knowing what happens to their data when it is processed by the company. While individuals claim to be concerned about how companies are handling their data, they actually do very little to combat those concerns in real life.[146] There is an argument that people are more cautious when the data concerns sensitive information, like health data, however, such individuals continue to use mHealth apps anyway despite there being a lack of strong privacy regulations in the United States. Therefore, rather than create completely new privacy laws, there could be an argument that the current system in place in the U.S. is sufficient enough to give consumers adequate peace of mind to continue to engage with mHealth apps, while simultaneously regulating companies on how they treat health data.

## CONCLUSION

While the concerns illustrated by critics of the GDPR are legitimate, it is imperative that the United States establishes a minimum baseline of protection for the privacy concerns of American citizens with a federal privacy law. As technology continues to advance, and people become more reliant on smartphones, telehealth, and personalized medicine, sensitive health information is put more at risk from inadequate security provisions of primary data controllers, third-party handlers, and from discrimination. This is especially concerning since the U.S. judiciary and legislative branches have recently made monumental decisions regarding healthcare. In a post-*Dobbs v. Jackson Women's Health Organization* world,[147] for example, some individuals that use menstrual-tracking apps, fertility-tracking apps, or any type of app that tracks one's location are worried that the potential information that these apps could provide may result in either public shaming or even criminal actions. This is not hard to imagine as data brokers have already been seen to sell information pertaining to when individuals visited a Planned Parenthood and included information in the sale regarding how long they stayed, from where they came, and where they traveled to after

---

[145] Mulder & Tudorica, *supra* note 89, at 266.
[146] Tanja Schroeder, Maximilian Haug & Heiko Gewald, *Data Privacy Concerns Using mHealth Apps and Smart Speakers: Comparative Interview Study Among Mature Adults*, 6(6) JMIR FORMATIVE RSCH. 1, 3 (2022).
[147] *Dobbs v. Jackson Women's Health Org.*, 142 S. Ct. 2228, (2022).

their visit.[148] Additionally, the leaking of personal health information from mHealth apps could affect an individual's ability to obtain a job, insurance, or monetary aid due to discrimination based on their data.[149] Therefore, a comprehensive federal privacy regulation must be implemented in the United States.

As previously mentioned, if States are concerned about the federal privacy law not affording enough protection, they should be able to enact additional provisions within their states to put those concerns at ease, especially with respect to sensitive data. It is not the ceiling of privacy protection that Americans should be concerned about; it is the floor. The United States must enact a minimum set of protections for its citizens that deals with privacy as a whole, not by acts here and there that tangentially allude to privacy concerns. This need is only more prevalent when taken into context with mHealth. mHealth app developers are not bound by centuries-old oaths of confidentiality. Rather, they are subjected to the whims and needs of computer-generated algorithms to develop personalized healthcare. These developers have access to millions of people's sensitive information which can easily be transferred with a simple sale. That is a lot of unrestricted power to have, thus there must be a governmental check on the actions of these mHealth app developers.

Ultimately, it is the federal government's responsibility to protect the rights of its citizens. With respect to mHealth and privacy, the only way this can be achieved is through federal privacy policies, similar to that of the GDPR. Not only will it be more efficient for American health

---

[148] Jay Edelson, *Post-Dobbs*, *Your Private Data Will Be Used Against You*, BLOOMBERG LAW: US LAW WEEK (Sept. 22, 2022, 4:00 AM), https://news.bloomberglaw.com/us-law-week/post-dobbs-your-private-data-will-be-used-against-you; *see also* Justin Sherman, *The Data Broker Caught Running Anti-Abortion Ads—to People Sitting in Clinic*s, LAWFARE (Sept. 19, 2022, 8:31 AM), https://www.lawfareblog.com/data-broker-caught-running-anti-abortion-ads—-people-sitting-clinics; *see* Holly Barker, *Nebraska Abortion Probe and Search Warrants for Data: Explained*, BLOOMBERG LAW (Aug. 12, 2022, 10:33 AM), https://www.bloomberglaw.com/bloomberglawnews/health-law-and-business/XABPUQAK000000?bna_news_filter=health-law-and-business#jcite (explaining Meta Platforms Inc.'s response to receiving warrants, which did not specifically mention abortions, to provide information about a woman suspected of committing a serious crime, which ultimately resulted in her and her daughter being charged with an illegal abortion in Nebraska).

[149] *See generally* Alexandra Heidel & Christian Hagist, *Potential Benefits and Risks Resulting from the Introduction of Health Apps and Wearables Into the German Statutory Health Care System: Scoping Review*, 8(9) JMIR MHEALTH & UHEALTH 1, 6 (2020) (detailing how chronically-ill individuals are worried that health insurance companies would discriminate against them if the insurance company were to access their health data).

providers, app developers, and consumers, but it will enable millions of people access to healthcare without sacrificing their right to privacy.