Guarding Health Data Privacy in Europe: The Limits and Challenges of Current Regulations

Christopher Borges, Ruth Cooper, Ashley Schuett, & Brandon Seehoffer

Executive Summary

Over the last several decades, digital technology has dramatically transformed healthcare. Mobile health tools, which consist of mobile applications and wearable technologies, are now common and present significant potential advantages, such as enhanced healthcare quality, expanded healthcare accessibility, and improved health-related habits. Many of these advantages are derived from the data that these technologies collect, analyze, and share. Wearable technologies, for example, are often equipped with an array of sensors capable of measuring environmental conditions (e.g., temperature and humidity), vital signs (e.g., heart rate and blood pressure), and behaviors (e.g., step-count and sleep patterns).

However, the dramatic increase in health data collection, particularly by for-profit entities, also presents serious risks. Mobile health apps often require users to divulge incredibly sensitive and intimate information, while even seemingly innocuous data can be utilized to infer personal information. Oura Rings, a smart ring used to track sleep and physical activity, can consistently identify when a woman is pregnant before they typically take a pregnancy test themselves. Biometric data as simple as step counts can be used to infer the movements and routines of individuals, and location data can be used to identify specific individuals with astonishing accuracy. A 2013 study found that 95 percent of individuals could be identified from their location data based on only four data points over four hours.

This data ultimately contains profoundly personal information about an individual, such as their sexual orientation, gender identity, mental health, genetic information, and lifestyle choices. Protection of this information is critical as individuals may face discrimination if it is revealed publicly. Discrimination based on sexual orientation has a long history, and Poland and Hungary recently passed laws curtailing the rights of LGBTQ+ individuals. Abortion is illegal in all cases in Malta and highly restricted in Poland. An activist in Poland is currently facing up to three years in prison for helping a woman access abortion pills. There is still tremendous stigma around mental health issues in many locales. Revelations of mental illnesses can lead to discrimination in housing and employment.

While the European Union has strong data protection and privacy laws such as the GDPR, these laws are not without limitations. This report identifies six specific limitations with the current EU data protection and privacy policy landscape:

- **Consent**: Even when individuals consent to the collection and processing of their health data, as required by EU law, they often have very little understanding of what they are consenting to and can be misled through dark patterns.

- **Transparency**: Systems are not consistently transparent about how the data they collect is utilized.
- **Enforcement**: Enforcement of the GDPR depends on member states' data protection authorities (DPAs), whose capabilities vary based on enforcement power and resources; therefore, GDPR enforcement varies throughout the EU. Strengthening the enforcement powers and resources of national DPAs could boost enforcement of GDPR and protect individual's personal health data.
- **Data Inferences:** By not specifically protecting data inferences, individuals are less able to assert their fundamental rights over their personal data.
- **Burden on Individuals:** A burden is currently placed on individuals to request access to data, interpret if laws are broken, and sue data companies in civil suits to protect their data. Collective action enabled by the GDPR and the Collective Redress Directive provide a better approach to hold data processors and data collectors accountable; however, assessment and compensation is inconsistent between Member States.
- **Information Security:** There are opportunities to improve the security practices of government and private companies to safely store people's sensitive health data.

Accordingly, we propose several policy recommendations to better protect individual's data and privacy:

1 Require health data collection agreements to have user-centric transparency with "opt-in" consent and appropriate enforcement by regulators.
2 Explicitly protect data inferences.
3 Require health apps and wearable devices to be certified by a recognized third-party organization.
4 Strengthen collective data rights through transparency and standardization efforts.

The GDPR demonstrates the capacity of the European Union to prioritize data protection and privacy. The collection and use of health data by private corporations makes privacy protections critically important. While the GDPR has many protections that also inherently include the protection of sensitive health data, limitations still exist. Taken together, the provided policy recommendations create comprehensive steps forward.

Introduction

Over the last several decades, digital technology has dramatically transformed healthcare. Mobile health applications, wearable devices, and various digital tools are now common and present considerable potential advantages, such as enhanced healthcare quality,[1] expanded

[1] Quinn et Al. "Cluster-Randomized Trial of a Mobile Phone Personalized Behavioral Intervention for Blood Glucose Control." *Diabetes Care* 34, no. 9 (July 19, 2011): 1934–42. https://doi.org/10.2337/dc11-0366

healthcare accessibility, and improved health-related habits.[2] At the same time, these technologies have revolutionized how health data are collected, analyzed, and shared in a way that existing data protection and privacy regulations have not foreseen. Health data, which includes sensitive information such as medical records, genetic data, and biometric data are among the most sensitive and private information that people generate. As a result, protecting health data and citizens' privacy has become an increasingly pressing concern for individuals and policymakers.

The protection and privacy of health data are crucial for a number of reasons. First and foremost, health data are deeply personal and sensitive, and individuals have a fundamental right to privacy with regards to this information. Breaches of health data can result in serious harm, including identity theft,[3] financial fraud,[4] and discrimination.[5] Second, the privacy and protection of health data are essential for maintaining trust in healthcare providers. Individuals must feel confident that their health data are being collected, stored, and shared in a secure and responsible manner. Without strong data privacy protections, people may be reluctant to share sensitive information with their healthcare providers, which can negatively impact their care and health outcomes.[6]

The collection of health data has expanded as digital technology has become increasingly pervasive in modern society. Wearable technology that collects biometric data is now common — tens of millions of Apple Watches and FitBits are sold annually.[7] Millions of individuals worldwide use mobile health apps for a variety of purposes,[8] which now constitute a multi-billion dollar industry.[9] Even more mundane uses of digital technology can result in the exposure of personal health data, such as conducting a web search for the symptoms of an illness or using a GPS navigation system for directions to a healthcare provider's office.

---

[2] Free et Al. "The Effectiveness of Mobile-Health Technology-Based Health Behaviour Change or Disease Management Interventions for Health Care Consumers: A Systematic Review." *PLoS Medicine* 10, no. 1 (January 15, 2013). https://doi.org/10.1371/journal.pmed.1001362.

[3] "Medical Identity Theft." World Privacy Forum. Accessed May 7, 2023. https://www.worldprivacyforum.org/category/med-id-theft/.

[4] Gee, Jim, Mark Button, and Graham Brooks. Rep. *The Financial Cost of Healthcare Fraud*. University of Portsmouth, January 2015. https://pure.port.ac.uk/ws/portalfiles/portal/1925942/The-Financial-Cost-of-Healthcare-Fraud---Final-%282%29.pdf

[5] *The New EU Regulation on the Protection of Personal Data: What Does It Mean for Patients?* European Patients Forum, 2020. https://www.eu-patient.eu/globalassets/policy/data-protection/data-protection-guide-for-patients-organisations.pdf.

[6] Lott, Bradley E, Celeste Campos-Castillo, and Denise L Anthony. "Trust and Privacy: How Patient Trust in Providers Is Related to Privacy Behaviors and Attitudes." *AMIA Annu Symp Proc*, March 4, 2020.

[7] Son, Woojin. "Global Smartwatch Shipments Grow 12% Yoy in 2022; Price Polarization Seen in Demand." Counterpoint Research, February 22, 2023. https://www.counterpointresearch.com/global-smartwatch-shipments-grow-yoy-2022/.

[8] Chan, Stephanie. "Mobile Wellness Apps Forecasted to Exceed 1 Billion Downloads in 2021." Market-Leading Digital & Mobile Intelligence. Sensor Tower, March 2021. https://sensortower.com/blog/mobile-wellness-market-trends-2021.

[9] Auxier, Brooke, Ariane Bucaille, and Kevin Westcott. "Mental Health Goes Mobile: The Mental Health App Market Will Keep on Growing." Deloitte Insights. Deloitte, December 1, 2021. https://www2.deloitte.com/xe/en/insights/industry/technology/technology-media-and-telecom-predictions/2022/mental-health-app-market.html.

Accordingly, health data are specifically regulated in many jurisdictions. In the United States, the Health Insurance Portability and Accountability Act (HIPAA) specifically protects health data in certain circumstances. In Australia, the Privacy Act provides extra protection around the handling of health data. In Canada, health data are protected by the Personal Information Protection and Electronic Documents Act (PIPEDA), along with additional laws in provinces such as Ontario, New Brunswick, and Newfoundland.

Nevertheless, while health data are frequently given special consideration, there are limitations with existing health data protection policies. For example, HIPAA in the United States only applies to data in clinical settings, research, and transmissions with health insurance providers; health data accessed through a smartphone, for example, is not protected.[10] Australia's Privacy Act was implemented in 1988 and therefore does not specifically address modern privacy concerns, such as targeted advertising.[11]

In the European Union (EU), health data are given special protection under the General Data Protection Regulation (GDPR). Article 9 of the GDPR states that "data concerning health," "genetic data," and "biometric data," must be held to a higher standard of protection.[12] However, while the GDPR is considered the "Gold Standard" of online data protection and privacy regulations, there are limitations with the EU's protection of health data and privacy given its more general approach compared to other countries' sectoral approaches.

This paper analyzes how EU data protection regulations protect health data collected by digital technology. Specifically, we focus on mobile health (mHealth), which is defined by the World Health Organization (WHO) as wearable technology and mobile apps used for health care.[13] The analysis highlights the strengths and weaknesses of EU health data protection and privacy laws, and offers policy recommendations to enhance them. Research for this paper was conducted through a literature review and interviews with health data protection and privacy experts.

The report is structured into five main sections. The first section defines "health data" for the purposes of this paper and reviews how wearable technologies and mobile apps collect health data. The second section details the risks associated with health data collection. The third section reviews the current privacy and data protection policies in the EU. The fourth section examines the shortcomings of those policies in the EU. The fifth and final section presents policy recommendations to strengthen health information privacy and data protections in the EU.

---

[10] "Protecting the Privacy and Security of Your Health Information When Using Your Personal Cell Phone or Tablet." Department of Health and Human Services, June 29, 2022. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html#footnote1_8n66xdq.

[11] "Targeted Online Marketing." Office of the Australian Information Commissioner. Accessed May 7, 2023. https://www.oaic.gov.au/privacy/your-privacy-rights/social-media-and-online-privacy/targeted-online-marketing.

[12] General Data Protection Regulation (GDPR). Art. 9 GDPR Processing of special categories of personal data. https://gdpr-info.eu/art-9-gdpr/.

[13] Alfawzan, N., M. Christen, G. Spitale, and N. Biller-Andorno. "Privacy, Data Sharing, and Data Security Policies of Women's Mhealth Apps: Scoping Review and Content Analysis." [In eng]. JMIR Mhealth Uhealth 10, no. 5 (May 6 2022): e33735. https://doi.org/10.2196/33735.

Background

Health Data

The definition of health data is contentious, particularly as data regarding many disparate activities can ultimately be related to an individual's health. In some situations, the relationship of an individual's data to their health is self-evident. For example, when a person goes to a doctor's office, the data collected by the doctor about their vital signs, symptoms, and medications are clearly health data. However, there are other situations where the relationship of data to an individual's health is less clear. Location data from a mobile device, for instance, are often not related to an individual's health, yet it can identify health information depending on the context. For example, if that same location data are used to track an individual while they are on a run, the individual's fitness level may be inferred. Furthermore, if the location data tracks an individual's travel to a hospital, therapist's office, or maternity clinic, the data are now clearly relevant to an individual's health. If the individual is visiting an oncologist's office based on the location data, one can infer this individual has cancer. During an interview, a healthcare ethicist defined health data as "any data that allows a 3rd party to make a reliable inference about your health status" to cover this broad range of scenarios.

Nevertheless, in practice, there are various definitions of health data. Per the McGraw-Hill Concise Dictionary of Modern Medicine, health data are "epidemiology information related to health conditions, reproductive outcomes, causes of death, and quality of life." However, legal definitions differ across jurisdictions. Australia has a broad definition of health data, which it defines as "any information about health."[14] In China, the National Health Commission defines "healthcare big data" as "healthcare-related data generated in the process of disease treatment [and] health management."[15]

Given our focus on the EU, this report uses "health data" as defined in the GDPR: "all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject."[16] This definition of health data is used to analyze how the GDPR protects health data collected by wearable technology and mobile health apps.

Health Data Collection

As highlighted earlier, there are many ways that health data can be collected outside of a patient's relationship with a healthcare provider and healthcare institution. This section highlights the two sources of health data in mHealth: wearable technologies and mobile health apps.

---

[14] "About health data in Australia." Australia Government, Department of Health and Aged Care. Web. Accessed May 11, 2023. https://www.health.gov.au/topics/health-data-and-medical-research/about-health-data.
[15] He, Zhicheng. "When Data Protection Norms Meet Digital Health Technology: China's Regulatory Approaches to Health Data Protection." *Computer Law & Security Review* 47 (November 2022): 105758. https://doi.org/10.1016/j.clsr.2022.105758.
[16] "Recital 35 Health Data*." Web. Accessed May 11, 2023. https://gdpr-info.eu/recitals/no-35/#.

Wearable Technology

"Wearable technology" is a broad term for technology products that individuals can wear on their bodies, such as activity trackers (e.g., Fitbit), smart watches (e.g., Apple Watch), and newer innovations like Google Glass. While wearable technology in a medical context has existed for some time, the commercial wearable technology market has exploded in recent years due to the emergence of fitness and wellbeing monitors. Today, wearable technology constitutes a multi-billion dollar industry — in 2022, the wearable technology market was valued at over $60 billion.[17]

Wearable technology's value largely stems from the data it gathers. Wearable technology is often equipped with an array of sensors capable of measuring environmental conditions (e.g., temperature and humidity), vital signs (e.g., heart rate and blood pressure), and behaviors (e.g., daily step-count and sleep patterns).[18] These data are incredibly valuable for healthcare providers, who can use it to gain valuable insights into their patient's health.[19]

Critically, the utilization of wearable technology will only continue to grow and the lines between a regulated medical device and a consumer wellness device will continue to blur.[20] Recent advancements in research suggest that a diverse assortment of wearable technology is likely to emerge in the coming years, including smart sport patches that can track hydration levels and smart contact lenses capable of detecting early indications of glaucoma.[21] In this context, the protection of data collected by wearable technology is increasingly critical.

Mobile Health Apps

Mobile health apps are software programs that provide health-related services, primarily through mobile phones and tablets. These apps consist of a wide range of physical health, fitness, and mental health-focused mobile applications, which include apps designed to treat or manage specific health problems such as opioid abuse and depression, self-management and tracking tools for health conditions, and access to medications and psychotherapy. Mobile health apps can

---

[17] "Wearable Technology Market Size, Share & Trends Analysis Report By Product (Head & Eyewear, Wristwear), By Application (Consumer, Electronics, Healthcare), By Region (Asia Pacific, Europe), And Segment Forecasts, 2023-2030." Grand View Research. Web. Accessed May 11, 2023. https://www.grandviewresearch.com/industry-analysis/wearable-technology-market.

[18] Kim, Jong Wook, Su-Mee Moon, Sang-ug Kang, and Beakcheol Jang. 2020. "Effective Privacy-Preserving Collection of Health Data from a User's Wearable Device" *Applied Sciences* 10, no. 18: 6396. https://doi.org/10.3390/app10186396.

[19] Liao, Y., C. Thompson, S. Peterson, J. Mandrola, and M. S. Beg. "The Future of Wearable Technologies and Remote Monitoring in Health Care." [In eng]. Am Soc Clin Oncol Educ Book 39 (Jan 2019): 115-21. https://doi.org/10.1200/edbk_238919.

[20] Brophy, Kieran, Samuel Davies, Selin Olenik, Yasin Çotur, Damien Ming, Nejra Van Zalk, Danny O'Hare, Firat Güder, and Ali Yetisen. "The future of wearable technologies." Imperial College London. Institute for Molecular Science and Engineering. June 2021.

[21] Ibid.

also monitor individuals' health and bodily functions, including physical activities, mood levels, stress, and sleep.

Given their function, mobile health apps unsurprisingly collect sensitive health data. To utilize a mental health app to treat depression, a user must share intimate details of their mental state and various behaviors. Mobile health apps can also track user location, which in turn can be used to identify individuals and infer characteristics about them.[22]

However, mobile health apps do not necessarily have rigorous privacy protection policies. A 2022 study which analyzed 578 mental health apps found that 33 percent did not have a privacy policy at all, and 44 percent shared personal health information with third parties.[23] A separate study of apps for depression and smoking cessation found that over 40 percent of apps transmitted data to third party services, but did not accurately disclose that practice in their privacy policy.[24]

Mobile health apps have greatly grown in popularity over the last several years, partially due to the increase in online activity driven by COVID-19.[25] Mobile health apps are now big business — the mental health app market alone was valued at over $5 billion in 2022.[26] In 2021 alone, Europeans downloaded over 280 million mobile health apps.[27] Mobile health apps will most likely continue to increase in popularity, especially due to the capabilities, convenience, and benefits they provide. For example, the WHO previously recommended using mobile health apps in rural and low income countries to improve access to healthcare.[28] Mobile health apps can also encourage healthy behaviors, offer personalized recommendations and feedback based on data, and can be a cost-effective way to monitor and manage health.[29]

---

[22] Morrison, Sara. "App trackers secretly sell your location data to the government. App stores won't stop them." Vox. February 23, 2021. https://www.vox.com/recode/22278402/x-mode-sdk-google-play-ban-location-data.
[23] Camacho, Erica, Asher Cohen, and John Torous. "Assessment of Mental Health Services Available through Smartphone Apps." JAMA Network Open 5, no. 12 (2022): e2248784-e84. https://doi.org/10.1001/jamanetworkopen.2022.48784.
[24] Huckvale, Kit, John Torous, and Mark E. Larsen. "Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation." JAMA Network Open 2, no. 4 (2019): e192542-e42. https://doi.org/10.1001/jamanetworkopen.2019.2542.
[25] Wortham, Jenna. "The Rise of the Wellness App." *New York Times*, February 17, 2021. https://www.nytimes.com/2021/02/17/magazine/wellness-apps.html.
[26] "Mental Health Apps Market Size, Share & Trends Analysis Report by Platform Type (Android, iOS), By Application Type (DepressionAnd Anxiety Management, Stress Management), By Region, And Segment Forecasts, 2023-2030." Grand View Research. Web. Accessed May 11, 2023. https://www.grandviewresearch.com/industry-analysis/mental-health-apps-market-report.
[27] Scacchi, Marco. "Health & Fitness App Installs in Europe Are Set to Reach 80 Million in Q1 2022." Sensor Tower. February 2022. https://sensortower.com/blog/state-of-health-and-fitness-europe-report-2022/
[28] World Health Organization. A practical guide for engaging with mobile network operators in mHealth for reproductive, maternal, newborn and child health. Geneva, Switzerland: World Health Organization; 2014.
[29] "5 Benefits of Mobile Health Apps in the Future." Designveloper. January 18, 2023. https://www.designveloper.com/blog/benefits-of-mobile-health-apps/

As the mobile health application market prepares for sustained growth, it is likely that more confidential health information will be gathered and managed by commercial entities. Given that data privacy and protection are fundamental human rights, individuals should have the ability to understand and control the collection, storage, and utilization of their personal health data, including who collects it and how it is used. To safeguard the sensitive health data of individuals, policymakers must make it a priority to comprehend the data protection and privacy safeguards that govern mobile health applications and how they are enforced.[30] Furthermore, it is critical to assess and minimize the risks associated with disclosing health data to mobile health companies to protect and defend the confidential health data of people.

Risks of Health Data Collection

> *"Health data is more valuable than credit card data. You can easily block a card, but health data is more robust."*
>
> - *Interview with EU digital policy expert*

Health data contains incredibly sensitive and intimate details. The data collected by wearable technology, for example, can determine many aspects of an individual's life. Fitness trackers and smartwatches can determine when an individual is beginning to fall ill.[31] Oura Rings, a smart ring used to track sleep and physical activity, can consistently identify when a woman is pregnant before they typically take a pregnancy test themselves.[32] Biometric data as simple as step counts can be used to infer the movements and routines of individualis, and location data, which are tracked by certain wearable technology, can be used to identify specific individuals with astonishing accuracy.[33] A 2013 study found that 95 percent of individuals could be identified from their location data based on only four data points over four hours.[34]

---

[30] Alfawzan, N., M. Christen, G. Spitale, and N. Biller-Andorno. "Privacy, Data Sharing, and Data Security Policies of Women's Mhealth Apps: Scoping Review and Content Analysis." [In eng]. JMIR Mhealth Uhealth 10, no. 5 (May 6 2022): e33735. https://doi.org/10.2196/33735.

[31] Ates, H. Ceren, Ali K. Yetisen, Firat Güder, and Can Dincer. "Wearable Devices for the Detection of Covid-19." Nature Electronics 4, no. 1 (2021/01/01 2021): 13-14. https://doi.org/10.1038/s41928-020-00533-1.

[32] Grant, Azure, and Benjamin Smarr. "Feasibility of Continuous Distal Body Temperature for Passive, Early Pregnancy Detection." PLOS Digital Health 1, no. 5 (2022): e0000034. https://doi.org/10.1371/journal.pdig.0000034.

[33] Yan, Tong, Yachao Lu, and Nan Zhang. "Privacy Disclosure from Wearable Devices." Proceedings of the 2015 Workshop on Privacy-Aware Mobile Computing, Hangzhou, China, Association for Computing Machinery, 2015.

[34] de Montjoye, Yves-Alexandre, César A. Hidalgo, Michel Verleysen, and Vincent D. Blondel. "Unique in the Crowd: The Privacy Bounds of Human Mobility." Scientific Reports 3, no. 1 (2013/03/25 2013): 1376. https://doi.org/10.1038/srep01376.

This data can be utilized to determine profoundly personal information about an individual, such as their sexual orientation, gender identity, mental health, genetic information, and lifestyle choices. This is alarming, as public knowledge of this information can lead to discrimination and other serious consequences. Examples include:

- **Sexual Orientation:** Queer individuals have a long history of facing discrimination, which continues to this day. For example, In 2021, lawmakers in Hungary approved legislation in 2021 prohibiting the sharing of content portraying homosexuality or sex reassignment with minors.[35] In Poland, the rights of LGBTQ+ individuals have been under assault for years, with several regions and municipalities announcing themselves "LGBT Ideology Free" in 2019.[36]
- **Women's Health:** Abortion is illegal in all cases in Malta and highly restricted in Poland — two EU member states.[37] Indeed, an activist in Poland is currently facing up to three years in prison for helping a woman access abortion pills, while legislators make abortion access more restricted.[38] The use of health data to track abortion is not unprecedented either - legislators in the U.S. state of Missouri recently revealed they had kept track of women's menstruation cycles to investigate any acts of abortion that might be revealed by this information.[39]
- **Mental Health:** There is still tremendous stigma around mental health issues in many locales. Revelations of mental illnesses can lead to discrimination in housing and employment and social rejection.[40]

What's more, the world is experiencing alarming democratic backsliding and undermining of democratic norms. In their 2023 report, V-Dem, an independent research institute, found that global democracy levels are back to their 1986 levels, and that more people now live in autocracies than democracies.[41] The report declared Hungary as an autocracy, and

---

[35] Pivarnyik, Balazs and Bela Szandelsky. "Hungary: Lawmakers pass law barring LGBT content for minors." AP News. June 15, 2021. https://apnews.com/article/government-and-politics-europe-hungary-laws-business-d093db541d1ad00bd4b28bb3a22 cdb1b.

[36] "Poland: Rule of Law Erosion Harms Women, LGBT People." Human Rights Watch. December 15, 2022. https://www.hrw.org/news/2022/12/15/poland-rule-law-erosion-harms-women-lgbt-people.

[37] "European Abortion Laws A Comparative Overview." Center for Reproductive Rights. Web. December 2020. https://reproductiverights.org/wp-content/uploads/2020/12/European-abortion-law-a-comparative-review.pdf

[38] "Poland: Prosecuting activist accused of aiding abortion 'sets a dangerous precedent'." Amnesty International. January 10, 2023. https://www.amnesty.org/en/latest/news/2023/01/poland-prosecuting-activist-accused-of-aiding-abortion-sets-a-dangerous-precedent/.

[39] Shipp, Laura, and Jorge Blasco. "How Private Is Your Period?: A Systematic Analysis of Menstrual App Privacy Policies." Proceedings on Privacy Enhancing Technologies 2020 (10/01 2020): 491-510. https://doi.org/10.2478/popets-2020-0083.; Mahdawi, A. (2019). If the government tracks women's periods, why not track male ejaculation, too? https://fortune.com/2014/08/27/how-max-levchins-glow-app-got-25000-women-pregnant/.

[40] Parcesepe, A. M., and L. J. Cabassa. "Public Stigma of Mental Illness in the United States: A Systematic Literature Review." [In eng]. Adm Policy Ment Health 40, no. 5 (Sep 2013): 384-99. https://doi.org/10.1007/s10488-012-0430-z.

[41] Democracy Report 2023. Defiance in the Face of Autocratization. V-Dem Institute. March 2023. https://www.v-dem.net/documents/29/V-dem_democracyreport2023_lowres.pdf.

Poland and Greece as democracies in steep decline. Just because a country is progressive and democratic today, does not mean that it will remain so tomorrow. The United States recently experienced this with the Dobbs decision which removed the right to abortion.[42] In Nebraska, police are using Facebook messages to investigate an abortion that occurred before the Dobbs decision was released.[43] Therefore, it is imperative to protect health data as there is no guarantee of what it may be used for in the future.

Ultimately, the reason why so much sensitive data relating to an individual's health is collected by private companies is for commercial purposes. Companies often use the data for targeted ads, despite limited evidence that targeted advertising produces superior results to contextual advertising.[44] During an interview with an EU consumer organization, targeted advertisements were noted as a big risk to individuals and urged that information related to health, medicine, and healthcare should be given by healthcare professionals, not companies.

As private companies collect more and more data, health data are more likely to be available and accessible to those with malintentions undermining citizens' data protection and privacy rights. As such, data protection and privacy laws must ensure they require the proper protections for the health data collected by private industry via wearable technology, mobile health apps, and other data collection methods.

European Union Protections

The foundation for EU health data protection and privacy, as with all types of data, lies in the Charter of Fundamental Rights of the European Union. This charter, proclaimed in 2000 and enforceable by the Treaty of Lisbon in 2009, establishes two pertinent articles. Article 7 grants EU citizens the "rights to [their] private and family life, home, and communications" and Article 9 grants the "right to the protection of personal data concerning [them]." Article 9 also requires data to be "processed fairly for specified purposes."[45] As such, EU privacy and data protection policies for health data stem from this framework.

The GDPR refined this framework to provide privacy and data protection laws that apply to data related to people in the EU. While the GDPR provides privacy and security to all personal

---

[42] Dobbs, State Health Officer of the Mississippi Department of Health, et. al v. Jackson Women's Health Organization et al. No, 19-1392. (Supreme Court 2022). https://www.supremecourt.gov/opinions/21pdf/19-1392_6j37.pdf.

[43] Kaste, Martin. "Nebraska cops used Facebook messages to investigate an alleged illegal abortion." NPR. August 21, 2022. https://www.npr.org/2022/08/12/1117092169/nebraska-cops-used-facebook-messages-to-investigate-an-alleged-illegal-abortion.

[44] Yeun Chun, Kwang, Ji Hee Song, Candice R. Hollenbeck, and Jong-Ho Lee. "Are Contextual Advertisements Effective?: The Moderating Role of Complexity in Banner Advertising." *International journal of advertising* 33, no. 2 (2014): 351–371.

[45] Regulation (EU) 2016/679, art. 9.

data, it lays out special considerations for specific types of data, including health data. **Table 1** identifies the types of data pertinent to our study and the associated legal protection. While most health data are covered by GDPR, anonymized health data does not receive the same level of protection as those covered in Article 9.

Table 1. Types of Data and EU Protection.

Type of Data	**Protection**
Personal Data	All of GDPR
Anonymous Data	Not covered per Recital 26, GDPR
Pseudonymous Data	Considered information on a natural person per Recital 26, GDPR
Genetic Data	Special category per Article 9, GDPR
Biometric data for purposes of uniquely identifying a natural person	Special category per Article 9, GDPR
Data concerning Health	Special category per Article 9, GDPR
Data Concerning a natural person's sex life or sexual orientation	Special category per Article 9, GDPR

Article 9 of the GDPR prohibits the processing of the types of data outlined in the table; however, the data may be processed if certain exceptions are met. Exceptions include if an individual "has given explicit consent to the processing of those personal data for one or more specific purposes;"[46] processing is necessary for carrying out an obligation required under employment, social security, and social protection law; processing has vital interests to the individual; and for purposes of preventative or occupational medicine. Member states may impose further limitations on the processing of health data.

While the GDPR remains the primary source of privacy and data protection for health data, other EU directives and regulations provide additional protections and considerations for health data. **Table 2** illustrates some pertinent laws that also apply to health data.

Table 2. Other Regulations Relevant for Health Data.

Law	**Pertinent Health Data Considerations**
GDPR	Processing of special categories of health data, such as health data, is prohibited with exceptions.
Data Services Act	Online platforms and online search engines must assess their risk from design, functioning or use on the protection of public health, minors, and serious negative consequences to a person's physical and mental well-being.

[46] *Ibid.*

	Consent required prior to the processing of personal data for targeted advertising.[47]
Digital Markets Act	The Commission grants an exemption to gatekeepers on the grounds of public health and allows the processing of personal personal data previously prohibited.[48]
ePrivacy Directive	Websites are required to obtain consent from visitors before retrieving or storing personal information, notably for cookies.[49]

The ePrivacy Directive is responsible for regulating the use of cookies, tags, and other tracking technologies, and it takes precedence over GDPR.[50] This means that any health data collected using cookies or tags must also adhere to the ePrivacy Directive. According to the ePrivacy Directive, non-functional cookies, like marketing or analytics cookies, require consent. As a directive, the ePrivacy Directive is implemented through national legislations, and thus, the regulations differ slightly in each Member State. For instance, the Netherlands doesn't mandate consent for analytics cookies that have minimal impact on an individual's right to privacy.[51] In the coming years, the ePrivacy Directive will be replaced by the ePrivacy Regulation, which aims to unify various EU Member States' legislations and broaden its definitions.[52]

In addition to the ePrivacy Regulation, the European Health Data Space (EHDS) is an upcoming legislation related to health data protection and privacy. EHDS is designed to be a "health specific ecosystem comprised of rules, common standards and practices, infrastructures, and a governance framework that aims at empowering individuals through increased digital access to and control of their electronic personal health data [and] providing a consistent, trustworthy and efficient set-up for the use of health data for research, innovation, policy-making and regulatory activities."[53] In the latest draft, EHDS plans to promote better exchange and access to different types of electronic health data, notably enabling the sharing of health data with third parties for secondary use (e.g. for research and the development of products and services, including AI). In addition, the legislation plans to ban health data to be used for commercial advertising, to develop dangerous products, and for any use against people.[54] This legislation is still being developed, but does contain risks to individuals' privacy, forcing doctors

[47] Regulation (EU) 2002/2065.
[48] Regulation (EU) 2022/192a5.
[49] Directive (EU) 2009/126/ EC.
[50] Cookies and the GDPR: What's Really Required?" iubenda. Web. Accessed May 11, 2023. https://www.iubenda.com/en/help/5525-cookies-gdpr-requirements
[51] Monhemius, Laura. "Health data and GDPR: Best practices for analytics in the EU." Piwik Pro. October 27, 2021. Updated April 12, 2023. https://piwik.pro/blog/health-data-and-gdpr/.
[52] Koch, Richie. "Cookies, the GDPR, and the ePrivacy Directive." GDPR.EU. Web. Accessed May 11, 2023. https://gdpr.eu/cookies/.
[53] "European Health Data Space." European Commission. Web. Accessed May 11, 2023. https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en.
[54] European Commission, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space" COM/2022/197 FINAL, May 3, 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0197.

to share patients data with the government as well as for-profit research without asking for their consent.[55]

Overall, the EU has enacted several laws that protect EU citizens and other persons' rights to data protection and privacy with their health data. While there are exceptions for health data that allow processing with fewer requirements, such as via the proposed EHDS, the GDPR still provides baseline protections that other countries do not have. Throughout EU law, consent proves a major theme and a limitation of EU policy that authorizes health data to be collected and processed when otherwise considered a special category.

Limitations of EU Data Protection and Privacy Policies

Despite the strengths of the EU's data protection and privacy legislation, the policy framework is not without limitations. This section highlights several issues with European protection of health data.

Consent

> *"Even though in theory a lot of personal data that is collected for online advertising, for example, is collected lawfully and then used lawfully, the way it is collected and the way companies ask for consent with cookie banners is so terrible and so misleading."*
>
> - *Interview with EU data privacy expert*
>
> *"There is consent in the formal sense but not in the meaningful sense. "*
>
> - *Interview with health data expert*

In the EU, organizations generally require consent before using cookies or processing health data. Article 6 of the GDPR notes that processing of personal data is considered lawful if "the data subject has given consent," among other conditions.[56] Obtaining informed consent safeguards individual privacy, autonomy, bodily integrity, and ethical principles. The GDPR defines consent and specifies it should be freely given, specific, informed, and unambiguous.

- **Freely given:** For consent to be freely given, it must be given voluntarily and not under pressure. The term "free" denotes that the person has the ability to make an actual choice,

[55] EDRi. "EU's proposed health data regulation ignored patients' privacy rights." EDRi. March 6, 2023. Web. Accessed May 11, 2023. https://edri.org/our-work/eu-proposed-health-data-regulation-ignores-patients-privacy-rights/.
[56] Regulation (EU) 2016/679, art. 6.

and any undue pressure or influence that may impact the decision renders the consent void..[57]

- **Specific**: For consent to be specific, it must be obtained specifically to the processing activities undertaken and not via a blanket consent. People should also be able to choose which types of data they give consent to share, versus the data they do not consent to share.
- **Informed**: For consent to be informed, people must have access to all the necessary information about how their data are processed, including who will have access, what it will be used for, and where it will be stored. Individuals should be made aware of their right to revoke their consent at any time, and the process for withdrawal should be as simple as the process for giving consent.
- **Unambiguous**: Finally, for consent to be unambiguous, it must be obvious that the individual has given consent to clearly defined actions. Merely acknowledging the terms and conditions is insufficient; individuals must provide an explicit indication of agreement. Consent must always be granted through an opt-in, declaration, or active gesture, leaving no room for ambiguity about the individual's consent.[58] Therefore, if mobile health apps use mechanisms such as checkboxes, they must not be pre-checked.[59]

While this is a strong definition of consent, in practice, it is not always adhered to. For example, for consent to be "freely given," mobile health apps should not use default opt-in boxes or other methods which may be coercive to obtain consent. However, experts at an EU consumer organization described how some mobile health apps require individuals to offer blanket consent to the use of data in order to utilize the app. Per a privacy lawyer we interviewed, "People have been conditioned to accept the terms and agreements, because there is something they want or need on the other side."

Further complicating the construct of "freely given" consent are "dark patterns"; this term refers to design features intentionally created to obscure, mislead, coerce, or deceive website users, resulting in unintended and potentially detrimental choices.[60] Dark patterns can be used to obtain consent from people for the use of their health data without their full understanding. Some mobile apps can utilize user interference design techniques (e.g., hiding important information in small print) that make it difficult for people to understand what they are consenting. Additionally, some mobile health apps can limit the options available to individuals through design choices like pre-selecting consent options or making it difficult to opt-out of data sharing. This can pressure people to give consent to share their health data, thereby making the consent no longer freely given. If individuals suspect that an app has used dark patterns to obtain their

---

[57] "GDPR Consent." Web. Accessed May 11, 2023. https://gdpr-info.eu/issues/consent/.
[58] *Ibid.*
[59] "Cookies and the GDPR: What's Really Required?" Web. Accessed May 11, 2023. https://www.iubenda.com/en/help/5525-cookies-gdpr-requirements.
[60] McNealy, Jasmine. "What Are Dark Patterns? An Online Media Expert Explains." August 3, 2021. Web. Accessed May 11, 2023. https://www.nextgov.com/ideas/2021/08/what-are-dark-patterns-online-media-expert-explains/184244/.

consent, they can report the app to the relevant regulatory body (e.g., their national DPA), but the onus is on the user.

Further, it is dubious that consent is consistently "informed," as individuals using these technologies are not always aware of what they are consenting to share. For example, research on menstrual self-management apps has shown that individuals often do not have full awareness of what their consent entails.[61] Additionally, a scoping review analyzing the most popular women's mobile health applications found that although all the apps collected health data, not all of them provided the option for individuals to give consent or read the privacy policy.[62]

As mentioned in the section on European Union protections, "data concerning health," "genetic data," and "biometric data" are held to a higher standard of protection than personal data under GDPR. In certain conditions, GDPR requires the individual to have given *explicit consent*. The term *explicit* pertains to the manner in which individuals convey their agreement and raises the standard of consent when there is a significant data protection risk.[63] Explicit consent under GDPR pertains to data processing and constitutes one of the mechanisms prescribed in GDPR to safeguard informational privacy. Explicit consent under GDPR comprises more criteria and conditions than informed consent; see **Table 3**.[64]

Table 3. Differences between informed consent, GDPR consent, and GDPR explicit consent.

[61] Shipp, Laura, and Jorge Blasco. "How Private Is Your Period?: A Systematic Analysis of Menstrual App Privacy Policies." Proceedings on Privacy Enhancing Technologies 2020 (10/01 2020): 491-510. https://doi.org/10.2478/popets-2020-0083.
[62] Alfawzan, Najd, Markus Christen, Giovanni Spitale, and Nikola Biller-Andorno. "Privacy, Data Sharing, and Data Security Policies of Women's mHealth Apps: Scoping Review and Content Analysis." *JMIR mHealth and uHealth* 10, no. 5 (2022): e33735–e33735.
[63] Kirwan, M., B. Mee, N. Clarke, A. Tanaka, L. Manaloto, E. Halpin, U. Gibbons, et al. "What Gdpr and the Health Research Regulations (Hrrs) Mean for Ireland: "Explicit Consent"-a Legal Analysis." [In eng]. Ir J Med Sci 190, no. 2 (May 2021): 515-21. https://doi.org/10.1007/s11845-020-02331-2.
[64] *Ibid.*

Informed consent [7]	GDPR consent [1]	GDPR explicit consent [1]
• Have received sufficient information in a comprehensible manner about the nature, purpose, benefits and risks of an intervention/service or research project • Not be acting under duress • Have capacity to make the particular decision	• Freely given—no imbalance of power, not conditional, granular, without detriment • Specific • Informed • Unambiguous • Unbundled • Active opt-in • Documented • Easy to withdraw • No blanket A valid GDPR consent depends on these cumulative criteria being present.	•The term "explicit consent" simply refers to the way GDPR consent is expressed by the data subject. It means that the data subject must give an express statement of consent. An obvious way to make sure consent is explicit would be to expressly confirm consent in a written statement.

SOURCE: Kirwan et al., 2021.[65]

This juxtaposition of e*xplicit consent* versus consent (for general personal data) has resulted in discussions regarding whether there exists a disparity between *unambiguous* and *explicit* consent, and if so, what characterizes that difference.[66] There is a general consensus that explicit consent for healthcare purposes necessitates the most robust forms of agreement, with the explicit uses of data specified when obtaining such consent. Moreover, health data consent may need to encompass scenarios involving several potential transfers of health data, including cross-border data transfers and cloud storage.[67] In one of our interviews, it was noted that transferring health data internationally is currently a challenge under GDPR.

Soon after the GDPR was implemented, there were still concerns about the effect of the regulation on consent. A study of the 500 most visited websites in each EU member state from 2017 to 2018 found that while the GDPR made the Internet more transparent (see Transparency section), there was still a scarcity of practical and user-friendly tools for individuals to authorize or refuse the processing of their personal data on the Internet.[68] Regarding mobile health

[65] *Ibid.*
[66] Rohatgi, Jitesh. "GPDR and healthcare: Understanding health data and consent." Pega. March 2, 2018. Web. Accessed May 11, 2023. https://www.pega.com/insights/articles/gdpr-and-healthcare-understanding-health-data-and-consent.
[67] *Ibid.*
[68] Degeling, Martin, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. "We Value Your Privacy ... Now Take Some Cookies." Informatik Spektrum 42, no. 5 (2019/10/01 2019): 345-46. https://doi.org/10.1007/s00287-019-01201-1.

applications, a study that assessed the disparities between an organization's data handling practices and the understanding of various individuals (e.g., privacy experts, legal scholars, and the general public) regarding those practices identified substantial levels of comprehension discrepancy in the privacy policies.[69] This finding suggests that such data policies can be misleading, especially for the general public. A separate investigation that specifically scrutinized menstrual cycle tracking applications found that none of the privacy policies "could be considered easy to understand".[70]

There is pending litigation related to consent currently in the European courts as well as previous cases. Currently, Commission Nationale de l'Informatique et des Libertés (CNIL) v. TikTok Technology Limited is pending before the French Administrative Court of Appeals. The French data protection authority (DPA) fined TikTok for violating the GDPR by failing to obtain adequate consent before collecting and processing personal data. In Google Ireland Limited v. CNIL, the case concerns the legality of Google's use of individuals' health data collected in the European Economic Area (EEA). The European Commission (EC) has fined Google €50 million for violating the GDPR by failing to obtain adequate consent before collecting and processing their health data. Google has appealed the EC's decision, and the case is currently pending before the Court of Justice of the European Union (CJEU).

Conclusion: **Even when people consent to the collection and processing of their health data, as required by EU law, they often have very little understanding of what they are consenting and can be misled through dark patterns.**

Transparency

"If patients don't feel like they have control of the data… it is a bad direction for society".

- *Interview with EU consumer rights organization*

For consent to be given, transparency is required. The concepts discussed in the previous consent section, particularly related to informed consent, are intertwined tightly with transparency. Under GDPR, organizations must ensure that personal information is processed lawfully and transparently. Accordingly, the definition of transparency is critical. Three goals of transparency have been identified: accountability, openness, and efficiency.[71] Accountability

[69] Reidenberg, J. R., Breaux, T., Cranor, L. F., French, B., Grannis, A., Graves, J. T., Liu, F., McDonald, A., Norton, T. B., and Ramanath, R. (2015). Disagreeable privacy policies: Mismatches between meaning and users' understanding. Berkeley Tech. LJ, 30:39.
[70] Shipp, Laura, and Jorge Blasco. "How Private Is Your Period?: A Systematic Analysis of Menstrual App Privacy Policies." Proceedings on Privacy Enhancing Technologies 2020 (10/01 2020): 491-510. https://doi.org/10.2478/popets-2020-0083.
[71] Ball, Carolyn. "What Is Transparency?" *Public Integrity* 11 (2009): 293 - 308.

creates an obligation to explain and justify conduct, openness creates trust, and efficiency is a product of understanding systems.

A challenge to transparency of informed consent is that privacy policies may not be available in a language that an individual understands. A research study found that although many apps offered multiple languages, the privacy policies were primarily in English, potentially resulting in individuals consenting without comprehending or reading the privacy policies.[72] For consent to follow the conditions described by GDPR, the consent process must be inclusive of individuals with varying backgrounds, abilities, and literacy levels. The individual's fundamental right to comprehend and access the information they are consenting to is essential and must be safeguarded.

Complaints made to DPAs argue that complex algorithms used by financial institutions, government agencies, and private corporations aren't transparent enough. Plaintiffs allege these systems produce unjustified disparate impacts, resulting from potentially biased training data. Courts will need to determine whether businesses should reveal more details about internal machine learning mechanisms or be allowed to keep trade secrets protected.

Data are used to create systems that are inherently not transparent, from recommendation algorithms on social media feeds to the digital advertising ecosystem. Further, even if engineers try to make these systems transparent, they may be unable. Real-time bidding for buying, selling and placing ads was found too complex to be transparent.[73] These ad systems, and many other automated decision-making (ADM) systems are considered black-boxes. GDPR gives the right of explanation to people subjected to these systems. However, the technical sophistication of these systems make them unexplainable, with researchers trying to find new ways to make them more transparent.[74] These systems should not be imposed on individuals with no way to opt-out when these mobile health applications and wearable technologies cannot meet GDPR's transparency requirement.

Conclusion: Systems are not consistently transparent about how the data they collect is utilized.

---

[72] Alfawzan, Najd, Markus Christen, Giovanni Spitale, and Nikola Biller-Andorno. "Privacy, Data Sharing, and Data Security Policies of Women's mHealth Apps: Scoping Review and Content Analysis." *JMIR mHealth and uHealth* 10, no. 5 (2022): e33735–e33735.

[73] Veale, Michael, and Frederik Zuiderveen Borgesius. "Adtech and Real-Time Bidding under European Data Protection Law." *German Law Journal* 23, no. 2 (2022): 226–56. doi:10.1017/glj.2022.18.

[74] Gryz, Jarek, and Marcin Rojszczak. 2021. "Black box algorithms and the rights of individuals: no easy solution to the "explainability" problem". Internet Policy Review 10 (2). DOI: 10.14763/2021.2.1564. https://policyreview.info/articles/analysis/black-box-algorithms-and-rights-individuals-no-easy-solution-explainability.

Enforcement

> *"It's good to do some strict enforcement on the big bad guys, because then the others notice. If you know things are enforced, then you behave according to the rules."*
>
> - *Advisor on Civil Liberties, Justice and Home Affairs*
>
> *"We don't want the industry to have an open bar for this data".*
>
> - *Interview with EU consumer rights organization*

The GDPR is enforced by DPAs in each EU member state, who have the power to investigate and impose fines for non-compliance with the regulation. The GDPR allows for fines of up to €20 million or 4 percent of a company's global annual revenue, whichever is higher.[75] However, the enforcement of GDPR has been criticized for being uneven and slow. Some countries have been more active in enforcing GDPR than others, with some critics arguing that some national DPAs lack the resources to fully enforce the regulation.

Additionally, some companies have been able to delay or avoid GDPR fines through legal challenges or by moving their operations outside of the EU. A research study examining the most prevalent mobile health apps designed for women discovered that these apps exhibit deficient data privacy, sharing, and security practices, and do not conform to the guidelines established by GDPR.[76] However, there has been little to no enforcement or repercussions for the companies that own these mobile health apps. While some member state's choose to enforce GDPR at different levels, such as the Irish Data Protection Commission (DPC), the European Data Protection Board (EDPB) has oversight.

Cross-border GDPR cases involving complaints against adtech business models and Google's location tracking have languished in regulatory limbo for years. DPC has faced the most criticism over its approach to GDPR, including opening up its "own volition enquiry" after a complaint to narrow its scope and avoid its crux. In recent months, the EDPB has "required the DPC to issue revised decisions."[77]

Strengthening the enforcement powers and resources of national DPAs could help enforcement of GDPR. Some critics have argued that some national DPAs lack the resources and

---

[75] "GDPR Fines/Penalties." Web. Accessed May 11, 2023. https://gdpr-info.eu/issues/fines-penalties/.
[76] Alfawzan, N., M. Christen, G. Spitale, and N. Biller-Andorno. "Privacy, Data Sharing, and Data Security Policies of Women's Mhealth Apps: Scoping Review and Content Analysis." [In eng]. JMIR Mhealth Uhealth 10, no. 5 (May 6 2022): e33735. https://doi.org/10.2196/33735.
[77] Hordern, Victoria. "Ireland's Approach to Enforcing the GDPR." Lexology, February 13, 2023. https://www.lexology.com/library/detail.aspx?g=d16aeb18-b731-4437-adef-8c57c111107c.

power to effectively enforce the GDPR. Strengthening their enforcement powers and providing them with more resources could help improve GDPR enforcement. There has been a movement to improve enforcement.[78]

The European Commission has committed to increasing its monitoring of how DPAs enforce the GDPR in EU member states. As part of this commitment, the commission will regularly request that national supervisory authorities provide it with reports on "large-scale" GDPR investigations every two months. Reports must include case numbers, the type of investigation, the DPA concerned, and "key procedural steps taken and dates." The commission will also report on the DPAs' reporting in its next application of the GDPR report. This monitoring may help to tackle the persistent criticisms of the GDPR's enforcement, which is often considered sluggish and ineffective, especially in the case of big tech companies..

Conclusion: **Enforcement of the GDPR depends on member states' DPAs, whose capabilities vary based on enforcement power and resources; therefore, GDPR enforcement varies throughout the EU. Strengthening the enforcement powers and resources of national DPAs could help enforcement of GDPR and protect individual's personal health data.**

Data Inferences

> *"If you have data about a specific person, and if you make an educated guess about another characteristic, then that is also personal data."*
>
> - *Advisor on Civil Liberties, Justice and Home Affairs*

A key difficulty in health data protection and privacy is how many disparate types of data can be used to infer information about an individual's health. In one famous example, Target, a large retail store, determined that an individual was pregnant before they realized it themselves by calculating a "pregnancy prediction" score based on their recent purchases.[79] While many of these purchases may have seemed innocuous, together they produced an accurate inference regarding deeply sensitive and personal health information about an individual. In this sense, data inferences are not personal data voluntarily provided by individuals, but are conclusions deduced from the voluntarily provided data.[80]

---

[78] Lomas, Natasha. "Big Changes Coming for GDPR Enforcement on Big Tech in Europe?" TechCrunch, January 31, 2023. https://techcrunch.com/2023/01/31/gdpr-enforcement-reform-dpa-oversight/.
[79] Hill, Kashmir. "How Target Figured out a Teen Girl Was Pregnant before Her Father Did." Forbes, October 12, 2022. https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/.
[80] Skiljic, Alina. The status quo of health data inferences, March 19, 2021. https://iapp.org/news/a/the-status-quo-of-health-data-inferences/.

In the context of wearable technology, data inferences using biometric data can reveal significant health information about an individual. Perhaps unsurprisingly, biometric data can accurately infer when an individual is suffering from an illness. A study published by smart ring-maker Oura openly advertised that their rings could detect the effects of COVID-19.[81] As these devices collect data on basic vital signs, it is clear that they would be able to detect signs of illness, which is sometimes marketed as a feature.

However, biometric data can be used to infer much more than just illnesses. For example, a 2022 study found that biometric data as seemingly innocuous as an individual's gait can not only be used to identify them personally, but also contains "health cues indicating the presence of a wide variety of physiological and behavioral health disorders."[82] Accordingly, a wearable technology company may be able to ascertain much more about an individual than the specific data the user agrees to share with them.

Despite the potential of data inferences to determine sensitive information about an individual, the GDPR does not specifically refer to data inferences in any capacity. Nonetheless, experts consider data inferences to be covered as personal data. In the UK, which has retained GDPR as domestic law after withdrawing from the EU, the Information Commissioner's Office explicitly states that "opinions and inferences are also personal data if the individual can be identified from that data, either directly or indirectly, and the information relates to that individual."[83]

Nevertheless, the lack of an explicit coverage of inferences under GDPR has its limitations. Much is left open to the interpretation of the CJEU, which is still developing a case body to establish legal precedents, making the current legal status of inferences puzzling at times. For example, cases addressing data inferences such as *YS, M and S v. Minister voor Immigratie, Integratie an Asiel* and *Peter Nowak v. Data Protection Commissioner* produced seemingly contradicting decisions on whether "personal data" includes "opinions, reasoning, and assessments that underlie" final inferred decisions.[84] That is, whether the inferences that lead to a final inferred result are personal data, and therefore given special protection. While this specific

---

[81] Pho, Gerald Norman, Nina Thigpen, Shyamal Patel, and Hal Tily. "Feasibility of Measuring Physiological Responses to Breakthrough Infections and COVID-19 Vaccine Using a Wearable Ring Sensor." Digital biomarkers 7, no. 1 (2023): 1–6.

[82] Ross, Arun, Sudipta Banerjee, and Anurag Chowdhury. 2022. "Deducing Health Cues from Biometric Data," Computer Vision and Image Understanding 221, 221: 103438. https://doi.org/10.1016/j.cviu.2022.103438.

[83] "Personal Data." Information Commissioner's Office. Accessed May 10, 2023. https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-for-the-use-of-personal-data-in-political-campaigning-1/personal-data/.

[84] Holder, Allan E. "WHAT WE DON'T KNOW THEY KNOW: WHAT TO DO ABOUT INFERENCES IN EUROPEAN AND CALIFORNIA DATA PROTECTION LAW." Berkeley technology law journal 35, no. 4 (2020): 1331–.

use case may appear trivial, the fact remains — the lack of specific protections on data inferences creates room for interpretation which may result in data receiving fewer protections.

Critically, while data inferences are generally recognized as covered by the GDPR, individuals nonetheless have fewer rights over data inferences compared to their data in practice due to the lack of specific protections. For example, individuals are less able to exercise their right to rectify, delete, and object to inferences, simply because they may not be aware that an inference had been made about them.[85] Although data processors are obligated to inform individuals about the data they collect, they are not required to disclose the inferences drawn from that data. Additionally, an individual's rights over their inferred data often require a more significant balance with the controller's interests, such as trade secrets, than their other personal data. A data controller may use an AI algorithm to make an inference, for example, and then claim the inference is protected intellectual property and, therefore, cannot be disclosed. As a result, the lack of specific safeguards for inferred data hampers individuals' ability to assert their rights over their personal data.

Conclusion: By not specifically protecting data inferences, individuals are less able to assert their fundamental rights over their personal data.

Burden on Individuals

> *"At an individual level, we do not have bargaining power. We accept the terms and conditions because we have no other choice. Data collectives allow users to pool and create some negotiating power, and also decide how they want to share for altruistic purposes."*
>
> - *Policy Expert*

In addition to the enforcement mechanisms previously discussed, civil suits prove a way for the average citizen to ensure their health data are properly collected, stored, and disposed per the GDPR. Today, civil actions for GDPR compliance are mostly commonly from individuals suing to hold data processors and data controllers accountable. For example, the infamous Schrems I and Schrems II cases, which invalidated the US-EU Safe Harbor Framework[86] and EU-US Privacy Shield[87] respectively, only had their impactful rulings since lawyer and data activist Maximillion Schrems sued Facebook. In "The Age of Surveillance Capitalism,"

---

[85] Wachter, Sandra, and Brent Mittelstadt. "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI." *Columbia Business Law Review*, October 5, 2018. https://doi.org/10.31228/osf.io/mu2kf.

[86] "Schrems I." The International Association of Privacy Professionals. Web. Accessed May 11, 2023. https://iapp.org/resources/article/schrems-i/.

[87] Fennessy, Caitlin. "The 'Schrems II' Decision: EU-US Data Transfers in Question." The International Association of Privacy Professionals. July 16, 2020. https://iapp.org/news/a/the-schrems-ii-decision-eu-us-data-transfers-in-question/.

Shoshana Zuboff describes the many obstacles faced when an individual requests their data. She concludes that there is an "insuperable burden placed on individuals" to challenge these injustices.

In general, there have been very limited number of civil actions, which is explained by "the lack of knowledge of data subjects and the limited damage caused to individuals."[88] Of course, individuals can request data from their data processors and data controllers; however, a longitudinal study has shown that access requests were only completed 50 percent of the time and many never responded.[89] Even if the details of the information collected are obtained, the individuals must know the information was collected illegally and then take it upon themselves to take action. Collective action lawsuits on the basis of data protection and privacy could properly convey the level of damage caused. Unfortunately, the data groups used by data processors may not always be known. Therefore, collective action lawsuits on the basis of data protection law are practically non-existent in Europe.

A collective approach would allow more success and greater opportunities for individuals to protect their rights through civil suits against data processors and data controllers. India serves as a potential model; they began developing a "community-based approach" which treats data as public goods to be managed by data trustees on behalf of communities. In this model, India defines the right to defend against a "collective harm," which is considered "when data is closed for public use and leads to welfare loss."[90]

EU law does allow collective action lawsuits for violation against GDPR. Article 80 of the GDPR grants individuals "the right to mandate a non-for-profit body, organization or association [...] to lodge the complaint [of rights infringement] on [their] behalf."[91] In 2020, EU Directive 2020/1828, also known as the Collective Redress Directive,[92] expanded collective action rights further by enabling cross-border claims and ensuring "at least one effective and efficient procedural mechanism for representative actions for injunctive measures and for redress

---

[88] Blok, Peter. "The Role of Private ACtors in Data Protection Law and Data Protection Practice." *Private regulations and enforcement in the EU: finding the right balance from a citizen's perspective.* Hart Publishing. 2020. Pg. 117.

[89] Kröger, Jacob Leon, Jens Lindemann, and Dominik Herrmann. 2020. "How Do App Vendors Respond to Subject Access Requests? A Longitudinal Privacy Study on IOS and Android Apps," ARES 2020: The 15th International Conference on Availability, Reliability and Security, , August. https://doi.org/https://doi.org/10.1145/3407023.3407057.

[90] "Report by the Committee of Experts on Non-Personal Data Governance Framework." Ministry of Electronics and Information Technology, Government of India. December 16, 2020. https://openfuture.eu/wp-content/uploads/2022/06/report-non-personal-data-governance.pdf.

[91] Regulation (EU) 2016/679, art. 80.

[92] "Injunctions Directive and Representative Actions Directive." European Commission. Web. Accessed May 11, 2023. https://commission.europa.eu/law/law-topic/consumer-protection-law/injunctions-directive-and-representative-actions-directive_en#.

measures is available to consumers in all Member States."[93] This directive is expected to empower entities to initiate collective action suits in relation to GDPR and other data protection and privacy laws, including the EU Cookie Act.[94] As this is a directive and the GDPR does not have criteria to assess recoverable damages, Member States must determine their processes and national standards for collective action through their respective DPAs. Therefore, collective action within the EU is inconsistent. For example, France only allows three types of associations to bring collective action suits, representative actions in Germany are limited to cease-and-desist measures and legal prerequisites of consumer claims, while the Netherlands allows for monetary compensation, but is subject to strict Dutch jurisdiction.[95]

Conclusion: A burden is currently placed on individuals to request access to data, interpret if laws are broken, and sue data companies in civil suits to protect their data. Collective action enabled by the GDPR and the Collective Redress Directive provide a better approach to hold data processors and data collectors accountable; however, assessment and compensation is inconsistent between Member States.

Information Security

[Large amounts of health data stored in one place will be] "huge honeypots for hackers".

- *Interview with EU digital rights organization*

Regardless of the quality of policies or their enforcement, the security of data is crucial. Data needs to be collected for many health systems to properly operate, data collection through health applications can enhance individual lives, and data collection can foster innovation, better patient care, and treatments. This data — at times — needs to be collected. That means its protection should be just as important. The GDPR imposes stringent regulations on the handling of health data, and non-compliance with these regulations can result in substantial penalties for organizations.

Even with these regulations, breaches still happen. In May 2021, Ireland's largest medical system, the Health Service Executive (HSE), suffered a major ransomware attack

[93] EUR-Lex. 2020. "Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on Representative Actions for the Protection of the Collective Interests of Consumers and Repealing Directive 2009/22/EC (2020)." EUR-Lex. 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2020.409.01.0001.01.ENG.

[94] Palazzi, Gloria. "Collective Redress Directive - implications for data protection law." LexisNexis. July 21, 2020.

[95] "Data class actions in Europe and spotlights in Mexico, Russia and the U.S." Hogan Lovells. March 12, 2021. https://www.hoganlovells.com/~/media/hogan-lovells/pdf/2021-pdfs/2021_03_12_data-class-actions-guide-2021.pdf?la=en

because of outdated devices connected to their network.[96] In February 2021, the Dutch DPA fined Amsterdam-based hospital OLVG because their records were insufficiently protected.[97] In 2022, the French DPA (known as CNIL) fined Dedalus Biologie €1.5 million for a data breach that exposed the health data of nearly 500,000 people.[98] The breach occurred when Dedalus Biologie extracted a larger volume of data than necessary during a software migration. In total, there have been 32 fines for "insufficient fulfillment of data breach notification obligations."[99]

Security concerns related to health data privacy and data protection, such as the incidents previously described, often correlate to the transferring and sharing of sensitive patient data between institutions and third parties. Information related to an individual's health can be disseminated to third parties through different means. For instance, the individual may share their health-related data with their doctor, insurer, family, and friends, similar to how other information is shared.[100] Additionally, personal health-related data can be shared in anonymized and aggregated forms for research purposes.

Security can not be reactive. Systems need to be secured so that these events and fines do not happen. Insufficient security practices of government and private companies are unacceptable. The potential harm of these breaches increases exponentially when it concerns individuals' health. If health data collection and retention is needed, it is essential that it is secure.

Conclusion: There are opportunities to improve the security practices of government and private companies to safely store people's sensitive health data.

---

[96] HSE Ireland (@HSELive). 2021. "There is a significant ransomware attack on the HSE IT systems. We have taken the precaution of shutting down all our our IT systems in order to protect them from this attack and to allow us fully assess the situation with our own security partners." Twitter, May 14, 2021, 2:28 a.m. https://twitter.com/HSELive/status/1393090933361623042.

[97] "Dutch Dpa Fines Olvg Hospital for Inadequate Protection of Medical Records ." Dutch DPA fines OLVG hospital for inadequate protection of medical records | European Data Protection Board, February 11, 2021. https://edpb.europa.eu/news/national-news/2021/dutch-dpa-fines-olvg-hospital-inadequate-protection-medical-records_en.

[98] "Health Data Breach: Dedalus Biologie Fined 1.5 Million Euros." Fildariane. Accessed May 10, 2023. https://www.cnil.fr/en/health-data-breach-dedalus-biologie-fined-15-million-euros.

[99] "GDPR Enforcement Tracker." list of GDPR fines. Accessed May 10, 2023. https://www.enforcementtracker.com/.

[100] Alfawzan, N., M. Christen, G. Spitale, and N. Biller-Andorno. "Privacy, Data Sharing, and Data Security Policies of Women's Mhealth Apps: Scoping Review and Content Analysis." [In eng]. JMIR Mhealth Uhealth 10, no. 5 (May 6 2022): e33735. https://doi.org/10.2196/33735.

Policy Recommendations

Recommendation 1: Require health data collection agreements to have user-centric transparency with "opt-in" consent and appropriate enforcement by regulators

In order to truly comply with GDPR's requirement for "freely given" consent, mobile health applications and wearable technologies should never use default opt-out boxes (e.g., boxes that are marked beforehand) or similar methods that may be coercive to obtain consent. These technologies should ask for consent in a way that allows users to opt-in and allows individuals to dive into the reasons for health data collection. There should also be stronger enforcement of mobile health apps that require individuals to offer blanket consent to the use of their sensitive health data in order to utilize the app. Additionally, the user-centric transparency and understandability of privacy policies is paramount, including what is collected, how it is used, and where it will be stored. Opt-in consent should be the norm in mobile health applications, as well as other health data collection methods, and should be easily accessible, readable, and offered in all languages that the technology offers.

Recommendation 2: Explicitly Protect Data Inferences

Clearly defining and safeguarding data inferences as personal information can help alleviate data protection and privacy concerns arising from judicial interpretations and a lack of awareness of inferences. For example, the California Consumer Privacy Act (CCPA) includes a definition of "personal information" that encompasses "inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."[101] An American privacy lawyer we spoke with commended the strength of the CCPA's coverage of data inferences.

Judicial opinions in California have reinforced the protection of inferences, as the initial opinion on the CCPA by the California Attorney General verified that inferences fall under an individual's "right to know" the data collected about them.[102] Accordingly, if an individual submits a request for a company to disclose the data collected on them, they must be made aware of any inferences that exist. Further, the burden of proof that inferences are indeed trade secrets is on businesses; it is insufficient to simply claim that they are. The Council of the EU and the European Parliament should expand GDPR to specifically cover data inferences so that EU citizens will receive stronger protections over how their personal data is used.

---

[101] California Civil Code §§ 1798.140.

[102] Office of the Attorney General State of California, Opinion of Rob Bonta, Rob Bonta. No. 20-303, California: 202. https://oag.ca.gov/system/files/opinions/pdfs/20-303.pdf

Recommendation 3: Require health apps and wearable devices to be certified by a recognized third-party organization

Requiring health apps and wearable devices to be certified by a recognized third-party organization (e.g. non-profit, government agency) would help ensure that these devices meet minimum safety and quality standards and that they protect consumer data. The certification could create requirements: that privacy policies are available in every language the app is available in, requiring technical controls such as end-to-end encryption, opt-in consent, and more fine-tune controls for transparency, and consent on the data collected and how it is used. This certification would allow people to know which apps and devices will provide privacy, security, and control over their sensitive health data. The European Parliament could implement this by leveraging and expanding on existing frameworks such as Label2Enable, which is already working to help individuals choose safe and effective apps.

Recommendation 4: Strengthen Collective Data Rights Through Transparency and Standardization Efforts

As more technology collects, tracks, and stores health data and biometric data in health and wellness apps, protecting individual rights becomes increasingly important. Damages to the individual are often limited; therefore, collective action suits serve as a comparatively stronger tool to ensure GDPRcompliance as damages are greater. Since the EU has seen mostly individual civil suits, the EU should take advantage of collective action efforts enabled by Article 80 of the GDPR and the Collective Redress Directive.

Collective action efforts are hindered by two main aspects: lack of knowledge and inconsistent assessment. The lack of knowledge is partly caused by access requests not being fulfilled with needed information to conduct civil action as previously discussed. Therefore, the EU and EU member states should ensure access requests are completed with the disclosure of data clusters or categorical variables so collective action suits may be formed. Since enforcement of GDPR and the Directive falls upon Member State laws, assessment of GDPR compliance will vary between Member States, which may lead to lack of consistent compliance and forum shopping. A standardized GDPR assessment at the EU level would ensure better and consistent protection of EU citizens' rights regarding their health data.