2022

Privacy Aspects of Direct-to-Consumer Artificial Intelligence/ Machine Learning health apps

Sara Gerke
Penn State Dickinson Law, sgerke@psu.edu

Delaram Rezaeikhonakdar

Recommended Citation

Sara Gerke and Delaram Rezaeikhonakdar, *Privacy Aspects of Direct-to-Consumer Artificial Intelligence/ Machine Learning health apps*, Privacy aspects of direct-to-consumer artificial intelligence/machine learning health apps, Intelligence-Based Medicine, Volume 6, 2022, 100061, ISSN 2666-5212, https://doi.org/10.1016/j.ibmed.2022.100061. *Privacy aspects of direct-to-consumer artificial intelligence/machine learning health apps, Intelligence-Based Medicine, Volume 6, 2022, 100061, ISSN 2666-5212, https://doi.org/10.1016/j.ibmed.2022.100061.* (2022).

Intelligence-Based Medicine 6 (2022) 100061

Contents lists available at ScienceDirect

Intelligence-Based Medicine

journal homepage: www.sciencedirect.com/journal/intelligence-based-medicine

Privacy aspects of direct-to-consumer artificial intelligence/machine learning health apps

Sara Gerke [a,*], Delaram Rezaeikhonakdar [b]

[a] Penn State Dickinson Law, 234 Lewis Katz Hall, 150 S. College St., Carlisle, PA, 17013, USA
[b] Penn State Dickinson Law, Carlisle, PA, USA

ARTICLE INFO

Keywords:
Privacy
Health
Apps
Direct-to-Consumer
Artificial intelligence
U.S. Law

ABSTRACT

Direct-To-Consumer Artificial Intelligence/Machine Learning health apps (DTC AI/ML health apps) are increasingly being made available for download in app stores. However, such apps raise challenges, one of which is providing adequate protection of consumers' privacy. This article analyzes the privacy aspects of DTC AI/ML health apps and suggests how consumers' privacy could be better protected in the United States. In particular, it discusses the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Federal Trade Commission (FTC) Act, the FTC's Health Breach Notification Rule, the California Consumer Privacy Act of 2018, the California Privacy Rights Act of 2020, the Virginia Consumer Data Protection Act, the Colorado Privacy Act, and the EU General Data Protection Regulation (2016/679 – GDPR). This article concludes that much more work is needed to adequately protect the privacy of consumers using DTC AI/ML health apps. For example, while the FTC's recent actions to protect consumers using DTC AI/ML health apps are laudable, consumer literacy needs to be much more promoted. Even if HIPAA is not updated, a U.S. federal privacy law that offers a high level of data protection—similar to the EU GDPR—could close many of HIPAA's loopholes and ensure that American consumers' data collected via DTC AI/ML health apps are better protected.

1. Introduction

The rapid development and use of Artificial Intelligence (AI)/Machine Learning (ML) in health care have brought not only enthusiasm but also ethical and legal challenges [1]. One of these challenges is providing adequate protection of the privacy of consumers who use AI/ML health applications addressed directly to them for their personal use (DTC AI/ML health apps). AI/ML is dependent on large amounts of data, and the use and disclosure of data like health data may compromise consumers' privacy. DTC AI/ML health apps are different from other DTC health apps in that they aim to discover patterns in big data—data characterized by the three Vs: volume, variety, and veracity [2]—to make predictions about the probability of disease or medical diagnosis [3]. In addition, unlike some other DTC apps, DTC health apps collect very sensitive data concerning a person's mental or physical health that need extra protection.

Over 318,000 DTC health apps are already available for users to download in app stores [4,5] some of which are based on AI/ML [6]. The health features that the Apple Watch provides to consumers for monitoring their heart rhythm is a popular example of the use of DTC AI/ML health apps in our daily lives [7,8]. Google also recently announced an "AI-powered dermatology assist tool," a web-based app planned to be launched soon that has the potential to diagnose 288 skin conditions [9]. However, the tech giant was heavily criticized for "biased sampling," using a training dataset consisting mainly of images from people with white skin and light brown skin [10]. In addition to the risk of bias in DTC AI/ML health apps, data privacy questions related to the collection, use, and sharing of data are becoming pressing. While there is a need to get innovations to market faster than ever before, there are additional risks of data breaches. According to the motto "fail fast and fix it later," developers may prefer to ignore data issues or solve them once the DTC AI/ML health apps are launched rather than missing the market opportunity [11]. It is important to promote innovation and the use of innovative technologies but not at the expense of consumers and their health data. Adequate protection of consumers' privacy also fosters trust in companies and can therefore positively impact app developers' revenues in the long term.

In this article, we will explore privacy concerns raised by DTC AI/ML health apps and suggest how consumers' privacy could be better protected in the United States (U.S.). Our suggestions may also be pertinent

* Corresponding author.
E-mail address: sgerke@psu.edu (S. Gerke).

https://doi.org/10.1016/j.ibmed.2022.100061
Received 14 December 2021; Received in revised form 27 February 2022; Accepted 29 March 2022
Available online 7 April 2022

for DTC health apps in general. We will first investigate whether the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides (adequate) protection to consumers' health information collected through DTC AI/ML health apps. We will show that HIPAA does not apply to health information collected through DTC AI/ML health apps in most cases. We will then discuss the U.S. Federal Trade Commission (FTC) Act and FTC's Health Breach Notification Rule. In particular, we will illustrate that the FTC has recently been paying close attention to whether DTC AI/ML health app developers keep their promises made to consumers and deal responsibly with health information. Lastly, we will look at recent legal developments at the U.S. state level—namely the California Consumer Privacy Act of 2018, the California Privacy Rights Act of 2020, the Virginia Consumer Data Protection Act, and the Colorado Privacy Act—and, for comparative purposes, the EU General Data Protection Regulation (2016/679 – GDPR).

We conclude that more efforts are needed to adequately protect American consumers' data collected via DTC AI/ML health apps. For example, while the FTC's recent actions to protect consumers using DTC AI/ML health apps are laudable, consumer literacy needs to be boosted. Congress also needs to act and create and pass a comprehensive privacy bill. New state privacy laws to improve consumers' data protection are commendable, but they add complexity for companies to comply with all applicable rules. A U.S. federal privacy law that offers a high level of data protection—similar to the EU GDPR—and preempts state laws with fewer privacy protections could tremendously simplify things. Such a law could close many of HIPAA's loopholes and ensure that American consumers' data collected via DTC AI/ML health apps are better protected. It could also likely make it easier to lawfully transfer data across borders between Europe and the U.S. in the future, thereby promoting innovation.

2. HIPAA and its loopholes

The HIPAA Privacy Rule is the leading national instrument in the U.S. that establishes standards concerning the use and disclosure of particular "individually identifiable health information" (named as "protected health information") [12,13]. In the context of DTC AI/ML health apps, however, HIPAA has several loopholes.

First, HIPAA only focuses on protected health information generated by so-called "covered entities" or "business associates." [1,14] The term "covered entity" exclusively applies to "a health plan," "a health care clearinghouse," and "a health care provider who transmits any health information in electronic form in connection with a transaction covered by" HIPAA [12]. Thus, DTC AI/ML health app developers are usually not considered covered entities, and health information collected through such apps fall outside of HIPAA's scope. This loophole stems from the fact that HIPAA was created at a time when data was generated in the conventional health care setting, such as hospitals, rather than also through DTC AI/ML health apps.

In a few cases, DTC AI/ML health app developers may be considered "business associates" under HIPAA. In general, business associates are persons or organizations that, on behalf of a covered entity, create, maintain, receive, or transmit protected health information for an activity or function regulated by HIPAA, such as claims processing, quality assurance, practice management, billing, and data analysis [12]. They are not members of the workforce of covered entities [12]. Business associates may also provide services, such as financial, administrative, management, legal, and data aggregation, to or for a covered entity, where the service provision includes the disclosure of protected health information [12]. Thus, if a DTC AI/ML health app developer creates protected health information on behalf of the covered entity, then such data is protected under HIPAA. In this case, the two parties must enter into a business associate agreement that contains appropriate safeguards for the protected health information [15]. The content and drafting of the business associate agreement play a vital role in determining for which data the DTC AI/ML health app developer is considered a "business associate." For example, manufacturers of cardiac devices, such as pacemakers or implantable cardioverter-defibrillators, are often *not* considered business associates under HIPAA concerning the *raw data* collected [16]. This is because the device manufacturers usually hold the raw data, and the business associate agreements generally only cover the data transferred to the hospitals or clinicians [16].

Second, even if DTC AI/ML health app developers may be considered "business associates" in rare cases, HIPAA exclusively covers protected health information. Thus, HIPAA may likely *not* protect all data collected through DTC AI/ML health apps. For example, some DTC AI/ML health apps may also collect non-health information, such as location data. Although such data may be sensitive because it allows inferences about the health condition of consumers (e.g., their COVID-19 risk), it falls outside of HIPAA's scope [14,17]. Moreover, "de-identified" health information is not individually identifiable health information and can be used and disclosed without limitations [13,18]. The de-identification standard can be satisfied through either the "Expert Determination" or the "Safe Harbor" method [19]. In a nutshell, the former method is a qualified statistician's determination, and the latter method is the removal of 18 types of identifiers, such as the individual's name and birth date [13,20].

Third, HIPAA's de-identification standard may not provide adequate privacy protection and can thus be regarded as another loophole [1,14]. HIPAA's ultimate goal to protect individually identifiable health information is not achieved when de-identified health information can easily be re-identified. For example, even if only de-identified health information collected through DTC AI/ML health apps is freely shared with or sold to other companies, such companies may have access to additional information with which they could effectively re-identify the de-identified health information.

This shortcoming of HIPAA was also shown in *Dinerstein v. Google* [21,22]. In this case, the defendants, the University of Chicago Medical Center and the University of Chicago, shared "de-identified" electronic health records, including those of the plaintiff Matt Dinerstein, with Google (also defendant) to create AI/ML-based predictive health models [21]. As an alleged HIPAA violation, the plaintiff underlined the problem of data triangulation, arguing that Google could effectively re-identify the records because it had access to huge amounts of other consumers' personal information, such as Google Chrome's web browsing history [21,22]. However, the District Court for the Northern District of Illinois granted the defendants' motions to dismiss, concluding that the plaintiff could not demonstrate damages for breach of contract [21]. This case underscores the difficulties for patients to successfully sue medical providers for sharing their health information with technology giants such as Google [23].

3. FTC Act and FTC's Health Breach Notification Rule

As one of its goals, the Federal Trade Commission (FTC) seeks to protect consumers from deceptive and unfair practices in the marketplace [24]. The FTC Act is the agency's primary statute. In particular, section 5(a) of the FTC Act bans deceptive or unfair practices or acts in or affecting commerce. Thus, the FTC also keeps a close eye on whether DTC AI/ML health app developers fulfill their promises to consumers and deal with health information responsibly [25]. For example, only recently, in June 2021, Flo Health has settled the FTC allegations made in a complaint first announced in January 2021 that the company violated section 5(a) of the FTC Act [26,27]. Flo Health collected detailed information about menstruations and gynecological health of more than 100 million female consumers with its Flo Period & Ovulation Tracker, a DTC AI/ML health app aimed at predicting ovulation and helping in pregnancy and childbirth [27]. Since 2016, Flo Health seemed to have acted in violation of its own promising privacy policies to keep consumers' personal health information secret and shared this sensitive data with third parties, including Google, Facebook, Flurry,

and AppsFlyer [27]. The FTC finalized order required Flo Health, among other things, to obtain the consumer's affirmative express consent prior to sharing their personal health information with third parties [26,28].

The FTC's Health Breach Notification Rule [29] may help to close HIPAA's loopholes, at least a little. This Rule applies to certain entities that HIPAA does not cover, such as vendors of personal health records—i.e., electronic records that contain individually identifiable health information received or created by health care providers and can be drawn from multiple sources [29,30]. These entities must usually notify the FTC and consumers in cases of a breach of unsecured identifiable health information ("breach of security"), such as cybersecurity intrusions or sharing consumers' sensitive health information without their authorization [29,30]. Due to the massive explosion in connected devices and health apps, the FTC issued a Policy Statement on September 15, 2021, to clarify the relevance and scope of the Health Breach Notification Rule [30]. In particular, the FTC explains that health app developers are considered "health care providers" under the Rule [30]. For example, according to this Policy Statement, the FTC's Health Breach Notification Rule may likely apply in a case where a DTC AI/ML blood sugar monitoring app collects consumers' blood sugar levels (health information) and their phone's calendar dates (non-health information), and the collected sensitive health information was disclosed without the consumers' authorization [30]. The FTC has so far never enforced the Health Breach Notification Rule but intends to change that in the future in light of the emerging field of health apps [30]. DTC AI/ML health app developers who do not comply with this Rule may thus face civil penalties in the amount of $43,792 per violation per day [29,30].

4. State privacy laws and the EU GDPR

To improve the privacy of consumers, California, Virginia, and Colorado have recently enacted comprehensive state laws. The California Consumer Privacy Act of 2018, which became effective on January 1, 2020, gives California consumers novel privacy rights over their personal information collected by businesses [31]. To further protect consumers' privacy rights, the California Privacy Rights Act of 2020 or Proposition 24 was approved by California voters on November 3, 2020, and amends the California Consumer Privacy Act [32]. In particular, it creates the California Privacy Protection Agency—i.e., an agency with complete administrative power, jurisdiction, and authority to implement and enforce both Acts [32]. Most California Privacy Rights Act's provisions will become effective on January 1, 2023. For example, the California Privacy Rights Act will extend the current right for California consumers to opt-out of sale of their personal information to a right to opt-out of *sharing* or sale of their personal information [33].

Virginia's Governor has also recently, on March 2, 2021, signed the Virginia Consumer Data Protection Act (SB 1392) into law, which will become effective on January 1, 2023. Like California's privacy laws, the Virginia Consumer Data Protection Act will give consumers personal data rights, such as the right against a controller to delete their personal data [34]. Colorado is the third state that has joined California's and Virginia's welcome initiatives to better protect consumers' privacy and enacted the Colorado Privacy Act (SB 190). This Act will take effect on July 1, 2023, and will also give consumers personal data rights, such as the right to data portability [35].

The new state privacy laws in California, Virginia, and Colorado do not apply to protected health information governed by HIPAA [36]. However, they help improve consumers' privacy by covering much of the health data created and used outside the clinical setting, such as through DTC AI/ML health apps.

All four state privacy laws were highly inspired by the EU General Data Protection Regulation (2016/679 – GDPR), which has been applied in all EU Member States since May 25, 2018 [37]. The GDPR contains wide-ranging rules concerning the natural persons' protection regarding the processing of personal data and concerning the personal data's free movement [38]. In comparison to HIPAA, the GDPR's scope is not limited to protected health information; instead, it generally applies to personal data processing [39]. The GDPR also adopts a broader approach towards "data concerning health," defined as "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." [40] Moreover, while the GDPR does not apply to anonymous information, it covers personal data that has undergone pseudonymization [41]. In general, in contrast to HIPAA, the GDPR offers more comprehensive privacy protection to individuals, including consumers using DTC AI/ML health apps.

5. Discussion and suggestions to better protect consumers' privacy

HIPAA cannot catch up with the rapid development of digital health technologies, including DTC AI/ML health apps. As seen, HIPAA is too narrow and has major loopholes. In most cases, HIPAA does not protect health information collected through DTC AI/ML health apps. Thus, one suggestion to better protect consumers' privacy could be to expand HIPAA's scope and eliminate the custodian requirement that HIPAA-covered entities or business associates must generate protected health information. Furthermore, the definition of "protected health information" is too tight. One solution could be expanding this definition to also cover non-health information that allows inferences about the health conditions of consumers. Lastly, HIPAA's de-identification standard does not offer enough protection in a world that is driven by big data and AI/ML. One approach could be that the agreement between the parties includes language requiring the party receiving the de-identified information to keep such information separately from other datasets and refrain from re-identification. Another approach could be that HIPAA gives up the de-identification standard as a privacy strategy altogether. For example, HIPAA could adopt the language of the EU GDPR and also apply to data concerning health that has undergone pseudonymization [40,41].

Even though having the FTC as an "enforcer" of privacy is helpful, the agency's current actions alone are likely not enough to adequately protect consumers' privacy. For example, the FTC acts and issues a complaint when it has "reason to believe" that the FTC Act has been or is being violated [25]. Thus, the privacy violation has likely already occurred in the moment of its actions. However, it is encouraging to see that the FTC has recently published guidance that contains suggestions for consumers on how to best select and use DTC health apps [25]. The agency also released FTC Best Practices for mobile health app developers to help them build security and privacy into their apps [42]. The FTC's recent announcement that the agency intends to enforce the Health Breach Notification Rule in cases of certain breaches by health apps is also a welcome attempt to promote better security and protection of consumers' individually identifiable health information [30]. However, much more work is still required to adequately protect the privacy of consumers using DTC AI/ML health apps. Those additional miles needed range from educational campaigns by agencies like the FTC to regulatory reforms that could, among other things, require developers of DTC AI/ML health apps to mitigate the privacy risks associated with those apps before they are made available to consumers. In particular, agencies like the FTC need to promote consumer literacy much more to enable consumers to better assess cyber and privacy risks and answer questions such as:

(1) What data is collected through DTC AI/ML health apps?
(2) For what purposes are the data collected, used, or shared (e.g., for model retraining or commercial purposes)?
(3) Is the data adequately secured against cybersecurity threats?

Moreover, although the privacy laws in California, Virginia, and Colorado are welcome instances of state-level attempts to close some of

HIPAA's loopholes, they have one significant weakness in common: They apply to residents of California, Virginia, and Colorado, respectively, and not to all Americans. They also significantly increase the complexity for companies to comply with all applicable privacy rules when developing DTC AI/ML health apps. Thus, having a federal law that adequately protects the privacy of all American consumers and preempts state laws with fewer privacy protections would enormously simplify things [43]. The GDPR could inspire the new U.S. federal law, which could have a broad scope covering the processing of personal data. The new law could be applied alongside HIPAA. Even if HIPAA is not updated, a U.S. federal law similar to the GDPR could plug many of HIPAA's loopholes and ensure that consumers' data collected through DTC AI/ML health apps are better protected across America. In addition, such a law would likely ease cross-border transfers of personal data between the U.S. and Europe. This is especially relevant in light of the recent *Schrems II* judgment, in which the Court of Justice of the EU struck down the so-called "Privacy Shield," a framework that had provided the possibility of lawful data transfer from Europe to the U.S [44,45]. While a recent announcement by the European Commission and the United States raises hopes for a new *Trans*-Atlantic Data Privacy Framework [46], a U.S. federal law similar to the GDPR would certainly promote data protection and further facilitate the sharing of personal data across the Atlantic.

6. Conclusion

The rapid development of DTC AI/ML health apps in the U.S. raises privacy concerns. DTC AI/ML health apps collect large amounts of sensitive data, and their use and disclosure may compromise the privacy of consumers. Much more work is needed to adequately protect the privacy of consumers using DTC AI/ML health apps, ranging from educational campaigns to regulatory reforms. For example, agencies like the FTC need to boost consumer literacy so consumers can better understand, among other things, for what purposes the data collected via DTC AI/ML health apps is used or shared (e.g., model retraining or commercial purposes). Even if HIPAA is not revised, a U.S. federal privacy law that provides an adequate level of data protection—similar to the EU GDPR—could close many of HIPAA's loopholes and ensure that American consumers' data collected via DTC AI/ML health apps are better protected. Such a law would also likely improve cross-border transfers of personal data between the U.S. and Europe.

Declaration of competing interest

The authors declare no competing interests.

References

[1] Gerke S, Minssen T, Cohen IG. Ethical and legal challenges of artificial intelligence-driven healthcare. In: Bohr A, Memarzadeh K, editors. Artificial intelligence in healthcare. London: Elsevier; 2020. p. 295–336.
[2] Zikopoulos P, deRoos D, Parasuraman K, Deutsch T, Corrigan D, Giles J. Harness the power of big data: the IBM big data platform. New York: McGraw-Hill; 2013.
[3] Babic B, Gerke S, Evgeniou T, Cohen IG. Direct-to-consumer medical machine learning and artificial intelligence applications. Nat Mach Intell 2021;3:283–7. https://doi.org/10.1038/s42256-021-00331-0.
[4] IQVIA. The growing value of digital health. https://www.iqvia.com/insights/the-iqvia-institute/reports/the-growing-value-of-digital-health. [Accessed 10 December 2021].
[5] Gerke S, Reichel C. Should we regulate direct-to-consumer health apps?. https://blog.petrieflom.law.harvard.edu/2021/09/01/direct-to-consumer-health-apps-regulation. [Accessed 10 December 2021].
[6] Chakraborty M. 10 best AI based healthcare apps you can try in 2021. https://www.analyticsinsight.net/10-best-ai-based-healthcare-apps-you-can-try-in-2021. [Accessed 10 December 2021].
[7] Letter from the FDA to Apple Inc.. https://www.accessdata.fda.gov/cdrh_docs/pdf18/DEN180042.pdf. [Accessed 10 December 2021].
[8] Letter from the FDA to Apple Inc.. https://www.accessdata.fda.gov/cdrh_docs/pdf18/DEN180044.pdf. [Accessed 10 December 2021].
[9] Bui P, Liu Y. Using AI to help find answers to common skin conditions. 10 December 2021, https://blog.google/technology/health/ai-dermatology-preview-io-2021; 2021.
[10] Feathers T. Google's new dermatology app wasn't designed for people with darker skin. 2021. https://www.vice.com/en/article/m7evmy/googles-new-dermatology-app-wasn't-designed-for-people-with-darker-skin. [Accessed 10 December 2021].
[11] Szabo L. A reality check on artificial intelligence: are health care claims overblown?. https://khn.org/news/a-reality-check-on-artificial-intelligence-are-health-care-claims-overblown. [Accessed 10 December 2021].
[12] 45 C.F.R. § 160.103.
[13] U.S. Department of Health and Human Services. Summary of the HIPAA privacy rule. https://www.hhs.gov/sites/default/files/privacysummary.pdf. [Accessed 10 December 2021].
[14] Price II WN, Cohen IG. Privacy in the age of medical big data. Nat Med 2019;25:37–43. https://doi.org/10.1038/s41591-018-0272-7.
[15] 45 C.F.R. § 164.502(e).
[16] Cohen IG, Gerke S, Kramer DB. Ethical and legal implications of remote monitoring of medical devices. Milbank Q 2020;98:1257–89. https://doi.org/10.1111/1468-0009.12481.
[17] Shachar C, Gerke S, Adashi EY. AI surveillance during pandemics: ethical implementation imperatives. Hastings Cent Rep 2020;50:18–21. https://doi.org/10.1002/hast.1125.
[18] 45 C.F.R. § 164.502(d)(2).
[19] U.S. Department of Health & Human Services. Guidance regarding methods for de-identification of protected health information in accordance with the health insurance portability and accountability act (HIPAA) privacy rule. https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html. [Accessed 10 December 2021].
[20] 45 C.F.R. § 164.514(a) and (b).
[21] Dinerstein v. *Google*. LLC, 484 F. Supp. 3d 561. 2020.
[22] Dinerstein v. Google. No. 1:19-cv-04311. 2019.
[23] Becker Jenna. Insufficient protections for health data privacy: lessons from Dinerstein v. Google. https://blog.petrieflom.law.harvard.edu/2020/09/28/dinerstein-google-health-data-privacy. [Accessed 10 December 2021].
[24] Federal Trade Commission. About the FTC. https://www.ftc.gov/about-ftc. [Accessed 10 December 2021].
[25] Federal Trade Commission. Developer of popular women's fertility-tracking app settles FTC allegations that it misled consumers about the disclosure of their health data. https://www.ftc.gov/news-events/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc. [Accessed 10 December 2021].
[26] Federal Trade Commission. FTC finalizes order with Flo health, a fertility-tracking app that shared sensitive health data with Facebook. Google, and Others, https://www.ftc.gov/news-events/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared. [Accessed 10 December 2021].
[27] Federal Trade Commission. Complaint 1923133. https://www.ftc.gov/system/files/documents/cases/flo_health_complaint.pdf. [Accessed 10 December 2021].
[28] Federal Trade Commission. Decision 1923133. https://www.ftc.gov/system/files/documents/cases/192_3133_flo_health_decision_and_order.pdf. [Accessed 10 December 2021].
[29] 16 C.F.R. Part 318.
[30] Federal Trade Commission. Statement of the commission on breaches by health apps and other connected devices. https://www.ftc.gov/system/files/documents/rules/health-breach-notification-rule/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf. [Accessed 10 December 2021].
[31] State of California Department of Justice. California Consumer Privacy Act (CCPA). https://oag.ca.gov/privacy/ccpa. [Accessed 10 December 2021].
[32] State of California Department of Justice. California officials announce California privacy protection agency board appointments. https://oag.ca.gov/news/press-releases/california-officials-announce-california-privacy-protection-agency-board. [Accessed 10 December 2021].
[33] Cal. Civ. Code § 1798.120.
[34] Virginia Consumer Data Protection Act, § 59.1-573.
[35] Colorado Privacy Act, § 6-1-1306.
[36] Cal. Civ. Code § 1798.145; Virginia Consumer Data Protection Act, § 59.1-572; Colorado Privacy Act, § 6-1-1304.
[37] GDPR, Art. 99(2).
[38] GDPR, Art. 1(1).
[39] GDPR, Art. 2.
[40] GDPR, Art. 4(15).
[41] GDPR, Recital 26.
[42] Federal Trade Commission. Mobile health app developers: FTC best practices. https://www.ftc.gov/business-guidance/resources/mobile-health-app-developers-ftc-best-practices. [Accessed 10 December 2021].
[43] Gerke S, Shachar C, Chai PR, Cohen IG. Regulatory, safety, and privacy concerns of home monitoring technologies during COVID-19. Nat Med 2020;26:1176–82. https://doi.org/10.1038/s41591-020-0994-1.

[44] Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems. Case C-311/18. ECLI:EU:C; 2020. p. 559.
[45] European Parliament. The CJEU judgment in the Schrems II case. https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf. [Accessed 10 December 2021].
[46] White House. Fact sheet: United States and European commission announce trans-atlantic data privacy framework. https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework. [Accessed 31 March 2022].