Journal of Law and Health

Volume 35 | Issue 3 Article

10-15-2022

Transcript: Presentation on Data Privacy Questions in the Digital Health World

Sara Gerke
Penn State Dickinson Law

TRANSCRIPT: PRESENTATION ON DATA PRIVACY QUESTIONS IN THE DIGITAL HEALTH WORLD

Presented By: Sara Gerke[1]

The Journal of Law and Health's
Digital Health & Technology Symposium

CLEVELAND-MARSHALL COLLEGE OF LAW
FRIDAY, APRIL 8, 2022

[1] Assistant Professor at Penn State Dickinson Law

The following is a transcription from The Digital Health and Technology Symposium presented at Cleveland-Marshall College of Law by The Journal of Law & Health on Friday, April 8, 2022. This transcript has been lightly edited for clarity.

Sara Gerke:

Thank you so much for having me. Today, I will discuss data privacy questions in the digital health world. I thought I would first give you an overview of the digital health landscape, and then we'll focus on the law – namely, the Health Insurance, Portability, and Accountability Act (HIPAA), the EU General Data Protection Regulation (GDPR), and the California Consumer Privacy Act of 2018 (CCPA).

Overview: Digital Health

Let's start with an overview of what's happening right now in the digital health landscape. First, we need to define what digital health means. There are different definitions of digital health, but the term is usually interpreted very broadly. The Food and Drug Administration (FDA) counts the following categories as digital health: mobile health (mHealth), health information technology (IT), wearable devices, telehealth and telemedicine, and personalized medicine.[2] I will mainly focus on mHealth and wearable devices.

Digital health is really booming right now, especially due to the COVID-19 pandemic. It has led to the adoption of digital health tools. This slide shows the estimated global digital health market size from 2019 to 2025. In 2022, the global digital health market was worth about 334 billion U.S. dollars, and it is expected to reach around $657 billion by 2025. This slide shows the projected U.S. mobile health apps market size from 2020 to 2030. As you can see, the mHealth Apps market is expected to increase continuously over the years. Medical apps make up the majority of the market, but fitness apps play a significant role as well.

One example of a digital health app is Ada, a symptom checker. Once you download the app, you answer a couple of questions about your symptoms. The app will then suggest the condition and offer advice. You can also monitor changes in your health. In addition, you can also receive heart health notifications on the Apple watch. Apple not only offers an electrocardiogram app, but it also has an irregular rhythm notification feature that notifies you if there's irregular heart rhythms, suggestive of atrial fibrillation.

The size of the U.S. portable medical device market is also projected to increase continuously over the next few years. In 2025, it is expected that the

[2] *What is Digital Health?*, U.S. FOOD & DRUG ADMIN., https://www.fda.gov/medical-devices/digital-health-center-excellence/what-digital-health (last visited Sept. 8, 2022).

biggest portion will be taken up by monitoring devices, which monitor vital signs such as temperature and respiration rate. That will then be followed by smartphone devices, which keep track of physical activities, followed by diagnostic imaging and therapeutics.

In 2021, Google also announced its intention to start a pilot study of a dermatology app that aims to help us better understand conditions affecting our skin, nails, and hair. Users can take photos with their smartphones, ask questions, and then get information about their possible conditions. However, this tool received considerable criticism because of the limited training data set, which was underinclusive of people with brown, dark brown, and black skin. This example of bias proves we need to make sure that we train algorithms on a very diverse data set.

Privacy Questions in Digital Health Landscape

Let's discuss some of the privacy questions in the digital health landscape. HIPAA is an abbreviation for the Health Insurance Portability and Accountability Act. Its privacy rule aims to protect health privacy by regulating the use and disclosure of certain health information.

The problem with HIPAA is that it does not adequately protect health information in the digital health world. The scope of HIPAA includes only protected health information generated by covered entities or their business associates. So what does that mean? In general, protected health information means individually identifiable health information. Covered entities are health plans such as health insurance issuers, healthcare clearing houses such as billing services, and most healthcare providers. A business associate is a person that performs certain functions or activities, such as data analysis, on behalf of an entity or provides services to a covered entity that involves the use or disclosure of protective health information (PHI). This means that HIPAA does not apply to health information generated by entities other than those covered by HIPAA.

For example, companies such as Amazon, Google, Microsoft, Facebook, and Apple are usually not covered entities under HIPAA's definition. This means that the health information collected by wearable devices and health apps is usually not protected under HIPAA. In some cases, companies like Apple and Google are business associates under HIPAA, as is the case if the companies are collecting protected health information through an app for a hospital. The business associate agreement between the parties usually regulates the details of this data collection and the data transfer.

Another shortcoming of HIPAA is the de-identification standard. De-identification is usually accomplished by stripping out 18 types of identifiers, such as the individual's birthdate or their name. Once the data is de-identified, it can be shared and used without violating HIPAA's boundaries. However, in the digital

health world, the privacy of individuals is not necessarily protected by the removal of these 18 identifiers. Companies like Apple and Google have access to a lot of data collected through their services, such as Google Maps. Carriers may be able to re-identify the de-identified data with one of their other data sets of 10. This issue is also known as data triangulation. The case of *Dinerstein v. Google* reflects the issue that re-identification is often not difficult for technology giants like Google to facilitate because they have other data sets on hand.[3] In the case of Google, they also had data from Google Maps.[4] The case was dismissed because Stein was unable to show damages, showing us quite plainly the challenges of successfully suing hospitals for sharing patient data with companies like Google.[5]

In contrast to the U.S., the World Health Organization (WHO) has implemented a much more comprehensive regulatory data protection framework. Namely, the EU General Data Protection Regulation, known as the GDPR.[6] The GDPR has a much broader scope than HIPAA. Under Section 1, the GDPR applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. The GDPR defines the term 'personal data' as 'any information relating to an identified or identifiable natural person, which is a so-called data subject.' 'Processing' is defined as 'any operational set of operation, which is performed on personal data, or on sets of personal data, whether or not by automated means, such as collection used for storage.' The GDPR also applies to data concerning health, which is defined under Article 4 Section 15 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. In addition to its wide material scope, the GDPR also has a very broad territorial scope. Under Article 3, the GDPR generally applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not. In some cases, the GDPR even applies to U.S. companies.

GDPR Provisions Addressing Personal Data

Under Article 3 Section 2, the GDPR applies to the processing of personal data of data subjects who are in the EU by controller or processor not established in the Union, where the processing activities are activities related to the offering of goods or services (paid or for free). This processing is irrespective of whether payment of the data subject is required for such data subjects in the EU, or the

[3] Dinerstein v. Google, Ltd. Liab. Co., 484 F. Supp. 3d 561 (N.D. Ill. 2020).

[4] *Id.* at 570.

[5] *Id.* at 590-92.

[6] Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, *available at* https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEC:32016R0679 [hereinafter GDPR].

monitoring of their behavior as far as their behavior takes place within the EU. For example, a U.S. company must comply with the GDPR in cases where the company deliberately monitors the behavior of data subjects who are in the EU with the help of health apps.

I would also like to highlight Article 9 of the GDPR. Article 9 Section 1 of the GDPR bans the processing of special categories of personal data. Special categories of personal data include data concerning health. However, Article 9 Section 4 of the GDPR contains some exception to this general ban, such as if there is an explicit consent of the data subject for one or more specified purposes, or if processing is necessary for reasons of public interest in the area of public health, such as protecting against cross-border threats to health (which was a relevant exception during the COVID-19 pandemic). The GDPR also contains many rights of data subjects such as the right to be forgotten, in Article 17, and the right to data portability, in Article 20.

In the U.S., we also see a trend at the state level to enact more comprehensive privacy laws similar to the GDPR. For example, the California Consumer Privacy Act (CCPA) of 2018 has been effective since January 2020.[7] The CCPA grants various rights to California residents with regard to personal information that is held by businesses. It is worth noting that the CCPA does not apply to HIPAA-covered, protected health information; however, it applies to personal health information that is collected outside of the traditional health setting, such as through health apps. The California Privacy Rights Act of 2020 has also recently been approved by California voters.[8] It will become effective in January 2023 and will also further expand California consumer privacy rights to the amendment of some of the CCPA's provisions. Colorado has also recently passed new comprehensive privacy laws,[9] and several other states may enact new privacy laws in the future.

[7] California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 (2018) (effective Jan. 1, 2020).

[8] *See The California Privacy Rights Act of 2020*, WEIL, GOTSHAL & MANGES LLP, https://www.weil.com/-/media/the-california-privacy-rights-act-of-2020-may-2021.pdf (last visited Sept. 8, 2022).

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