Health Data Privacy in a Digitized World

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Wei Wang
Spring, 2021

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signature  Date 05/07/2021
Wei Wang

Approved _____ Date _____
Sharon Tsai-hsuan Ku, Department of Engineering and Society

Introduction

Current smartwatch and smartphone technologies enable people to track specific health data, such as heart rate, and sleep quality. This data can be used to help people build healthy daily routines. However, despite the convenience provided by these new technologies, they also create new security and privacy issues, such as possible improper usages of users' health data. According to the U.S. Consumer Privacy Index 2016 provided by the TRUSTe/National Cyber Security Alliance (NCSA), a nonprofit organization promoting cybersecurity and privacy awareness, 68% of the population were concerned about their data privacy, whereas only 57% were worried about losing their primary source of income (*TRUSTe National Cyber Security Alliance U.S. Consumer Privacy Index 2016 Infographic* 2016).

Health data is crucial when it comes to public health management. For example, this data can be analyzed to reveal insights regarding the prevention of potential health crises. With the advancement of technology and analytical techniques, health data collection has become more convenient. Health professionals may be utilizing new technologies like smartphones and wearables to closely monitor their patients' health status in real-time and advanced data analysis techniques can help to detect issues earlier. However, there are privacy concerns and risks involved with these devices and technologies. Traditionally, health data is collected by healthcare service providers and other related organizations, including hospitals and health insurance companies. These organizations and their business associates are regulated by the HIPAA and HITECH act, which list the privacy and security practices that must be strictly followed (Health Insurance Portability and Accountability Act of 1996 (HIPAA) | CDC, 2018; HITECH Act Enforcement Interim Final Rule, 2017). However, with new technologies,

organizations like technology companies may also collect and access this type of data. The participation of these new actors in the health data network has introduced new issues and concerns regarding data privacy and security.

Research Question

Privacy in a digitized world is essentially the right of users to determine "who can access what data about me, where, when, and for what purpose" (Newman, 2019). Since information is stored and collected virtually, it is more difficult to prevent and track any unauthorized access. Additionally, some data may not be considered health data but can be used to derive health information with advanced data analysis methods. For example, in 2017, Facebook created an algorithm to analyze users' mental health from social media posts (Goggin, 2019). With more health data collected and created by organizations outside of the healthcare industry, it is difficult to determine the legal ownership of this data. However, more health data can lead to better health management and risk prevention. To better understand the concept of health data privacy in the digital age, it is essential to answer the following two questions: are technology companies required to comply with HIPAA like healthcare organizations, and how does the participation of technology companies change the notion or interpretation of health data privacy.

Literature Review

Within the past ten years, numerous studies have been done to learn the various forms of privacy risks regarding health data in a digitized world. This data is usually collected from a variety of platforms, including social media and wearable devices. Most of these studies are

focused on privacy issues with current technologies; however, very few are considering the possible new problems introduced by the evolution of these technologies in the future.

Throughout these studies, several common themes appeared consistently. For example, several research projects analyzed the users' awareness of the privacy risks involved with using wearable health devices or other health software and applications. These studies often look at whether users understand the privacy conditions that they approved and whether companies have purposely included specific terms that would enable them to use data in their interests (Al Ameen, Liu and Kwak, 2010; Raij, Ghosh, Kumar and Srivastava, 2011; Paul and Irvine, 2014; Obar, 2015; Ostherr et al., 2017; Gostin, Halabi and Wilson, 2018). In some cases, the technologies or methodologies have been developed recently, and the users and service providers may not fully realize their privacy risks (Motti and Caine, 2015). Flaws within a technology may lead to serious privacy concerns. Many research projects have analyzed the technologies involved with wireless communication between different devices and evaluated their security (Zhou and Piramuthu, 2014; Ching and Singh, 2016).

Regulatory agencies and governments' roles in data privacy protection is another focus in many studies. Some groups have analyzed the current regulations and law systems to understand the authority’s efforts to ensure the confidentiality of consumer data (Van Dijck and Poell, 2016; McDermott, 2017). Another perspective looked at scenarios where the government has become a source of privacy issues (Vezyridis and Timmons, 2017). Lastly, modern data analysis methods allow organizations to infer users' mental health state based on their social media activities. One research project has been done to study the ethical tensions and other related social problems involved with such practice (Chancellor et al., 2019).

Most of these studies and research projects have analyzed user-health data privacy issues from many different perspectives and focused on various stakeholders. One common conclusion that can be drawn from these analyses is that it would be impractical to rely on users to control the privacy of their data in most cases. One study stated that data privacy self-management is a fallacy and practically impossible as users would often accept service terms and conditions without a complete understanding (Obar, 2015). Consequently, it will be necessary for the government and regulatory agencies to step in and prevent certain actions against user data privacy and security. An example of the government's effort to protect consumer data privacy is the California Consumer Privacy Act (CCPA), which has become effective on January 1, 2020. This act enhances the consumer privacy rights of California residents by allowing them to request deletions of their data stored by businesses and their affiliates (Dean, 2020).

Research studies have also suggested that as technology improves over time, the privacy and security model will evolve. As a result, more advanced standards should be created to encounter these changes. These standards may be new regulations or more advanced technical procedures that will bring security to a new level.

These studies provide a useful framework for developing the proper privacy and security practices for current technologies and systems. However, these technologies will evolve quickly; new systems may be designed and used for data sharing and applications. It would be critical to consider these possibilities and methods that can be used to encounter these changes.

STS Framework and Method

The SCOT (social construction of technology) theory will be used to study the privacy issues involved with current mobile and wearable health technologies. This STS framework

allows researchers to study the impacts of the relevant technologies on various social groups and provides helpful insights into the different interests of each social group. In this study, the relevant social groups are determined to be healthcare providers, technology companies and manufacturers, patients and users, and the government. Consumers are the source of data, and companies create the technologies used by the consumers. Government helps to regulate the privacy of certain data. The different interests of each social group may result in conflicts. For example, companies may use the data collected for advertising purposes while users may want to ensure their data privacy rights. An important goal of the SCOT analysis is to identify the possible conflicts and propose temporary or permanent solutions to counter these issues.

During this research, various government documents relating to health data regulations and the privacy policies of different technology companies will be analyzed. This analysis will provide useful insights regarding these organizations' views on health data privacy. Additionally, a survey will be created and distributed among the general population to collect users' and consumers' opinions on this topic. Lastly, interviews will be conducted with members of healthcare organizations, such as doctors.

In addition to SCOT, the theory of surveillance capitalism will be used to analyze the ethical issues introduced by the new technologies. Surveillance capitalism is an economic system where personal data is the commodity for profit-making. The commodification of personal health data is one of the most likely issues involved with data privacy; thus, Surveillance capitalism will be suitable and relevant for this study.

Data Analysis

Government and Regulations

Government is an important stakeholder in this study as legislative regulations are crucial when it comes to data privacy. The current regulation that protects patients' health data privacy is the Health Insurance Portability and Accountability (HIPAA) Act of 1996, which prevents covered entities from using patient health data in unauthorized ways (Health Insurance Portability and Accountability Act of 1996 (HIPAA) | CDC, 2018). The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted in 2009, has extended the protections offered by HIPAA to electronic patient data, but the criteria of the covered entities have remained unchanged (HITECH Act Enforcement Interim Final Rule, 2017). However, over the course of the past 10 years, the development of new technologies has enabled more organizations to collect digital personal health data, and many of these organizations are not considered covered entities under HIPAA's rules (Bari and P. O'Neill, 2019; Gostin, Halabi and Wilson, 2018).

As established by HIPAA, only the health care providers, health insurance providers, and any business associates of the previous two types are legally required to follow the privacy practice standards established (Health Insurance Portability and Accountability Act of 1996 (HIPAA) | CDC, 2018). However, in today's digital world, the types of health data collectors and managers have expanded far beyond these covered entities. Most noticeably, the introduction of smartphones and smart wearable devices has resulted in a more convenient way to collect personal health data and a growing amount of health management apps. Additionally, the growth of social media platforms also enables organizations to analyze users' health status more accurately from the posts created. The development of these technologies and platforms has led to an increasing amount of health data managed by sectors outside of HIPAA's governance.

Thus, current regulations are insufficient to safeguard users' rights to their health data privacy (Bari and P. O'Neill, 2019).

In addition to the limited criteria for the covered entities, HIPAA also only protects a specific category of information. HIPAA only regulates protected health information (PHI). This type of information is defined as any data relating to an individual's physical and mental health history, the provision of healthcare services to the individual, or any payment information acquired for the healthcare services. Any de-identified information will not be protected under HIPAA's rules (Health Insurance Portability and Accountability Act of 1996 (HIPAA) | CDC, 2018). As a result, the application of de-identified data is unrestricted; however, with current data analysis methodologies, it is possible to recover personal information from these de-identified data (Lubarsky, 2017).

Although the current federal regulations can only provide limited protections to personal health data privacy, there has been a recent state statute with more comprehensive consumer privacy rights in the digital age. The California Consumer Privacy Act (CCPA) has provided extensive rights to consumers residing in the state of California over personal information collected and managed by businesses. Under this law, consumers will be acknowledged of any personal data collected by a covered entity and how this information will be utilized. Consumers will also have the right to delete any information collected from and prevent the selling of their data. The act has a broad definition for personal information, including most data about an individual that is not publicly available from government records (Bari and P. O'Neill, 2019; California Consumer Privacy Act (CCPA), n.d.). Thus, health and any medically related information are protected. Additionally, organizations that are required to comply with CCPA are for-profit companies, which are not entities covered by HIPAA. This act can only benefit the

residents of California; however, it can serve as a fundamental framework for a new federal privacy regulation or an extension to HIPAA.

Since most states do not have privacy laws similar to CCPA, the majority of the American population still lack legal protection of their data privacy from organizations outside of HIPAA's covered entities (Rippy, 2021). As a result, their privacy rights rely heavily on the privacy policies designed by these organizations; it is necessary to examine these policies to understand their attitudes toward users' privacy.

Businesses and Technology Companies

Fitbit is a popular wearable device currently in the market. In its privacy policy, there is no clear definition nor distinguishment for health data; thus, it is difficult to determine whether medically related data will be treated indifferently with other types of personal information. Fitbit also allows its users to share any personal information with third-party apps, but Fitbit does not have any privacy requirements for these third-party apps, and shared data is no longer protected by Fitbit's privacy policy. Additionally, Fitbit shares information collected with its business associates and partners for data processing and analysis purposes. Any shared data in this case still has its privacy ensured by Fitbit's policy. Lastly, Fitbit provides more terms and protections for users residing in California as required by CCPA (Fitbit Legal Privacy Policy, 2020). Overall, Fitbit does not provide strong protection for users' health data as this information is treated indifferently with others.

Apple is another major provider in the personal wearable device market and the smartphone market. Both technologies are heavily involved with digital health data collection. In Apple's privacy policy, health data is explicitly defined to be "data relating to the health status of an individual, including data related to one's physical or mental health or condition." Apple also

considers any personal data that can be used to infer or detect an individual's health status as health data. However, data that falls under such criterion is difficult to determine, but it effectively broadens the scope of health data defined by Apple. Furthermore, any data collected and managed by the Health app on Apple devices are protected by end-to-end encryption. This protocol prohibits anyone other than the user to access his or her data, which greatly enhances both the security and privacy of user information. This protection can be invalidated if the user decides to share any part of his or her health data with Apple or another third-party software. Apple affirms that any health data shared by the users will only be used to feature improvement and development purposes, and the data will be de-identified to reduce privacy concerns. However, it is beyond Apple's ability to ensure user privacy if the data is shared with third-party apps. Although Apple requires any partnering third-party to have a privacy policy to reduce the risk of privacy infringement, the strength and strictness of the policies may vary greatly. Like Fitbit, Apple also provides additional terms for California customers due to CCPA (About the privacy and security of your health records, 2019; Legal - Apple Privacy Policy - Apple, 2020).

Since many device manufacturers allow their users to share personal data with third-party apps, it is important to also study these organizations' privacy policies and determine whether there pose any significant risks. Sleep Cycle is a popular app available on both iPhone and Android devices. This app utilizes sleep data collected from users' devices to track and analyze their sleep patterns and help them develop healthier habits. In Sleep Cycle's privacy policy, it states that information collected from the users may be shared with business partners for analytics and advertising purposes. The types of information that may be shared are not specified, which means that health data may be included. Additionally, Sleep Cycle claims that aggregated or de-identified information may be shared publicly or with third parties (Privacy

Policy - Sleep Cycle alarm clock, 2018). With de-identification may help to significantly reduce the level of privacy concerns, it is possible to re-identify the information. Studies have shown that if any personal information is anonymized at an insufficient level, it is still very likely to re-identify the data using modern techniques (Lubarsky, 2017). As the level of de-identification is not specified in Sleep Cycle's privacy policy, there may still be privacy issues involved.

The level of privacy protections for users' health data varies greatly among the companies, and device manufacturers do not always offer more security than third-party apps. Additionally, businesses such as Fitbit have utilized certain data to analyze users' interactions with their services and create personalized advertisements. Although the data used may not reveal any health information; however, users' interactions with health-related functions would often generate other types of data, which may be used for analytical and advertising purposes. Such practices have allowed businesses to commodify their users. Users must carefully examine the privacy policies of their service providers to determine whether it would be relatively safe to share their personal information and utilize the provided services.

Consumers and Users

The opinions of the public, especially users of relevant devices and services, can greatly influence the decision-making of both companies and the government. Thus, a health data privacy survey has been conducted to understand their opinions. There has been a total of 32 respondents, and 18 of them have been using a device to track their health status regularly. According to the survey results, a slightly higher number of users are concerned about their privacy related to the device manufacturers than to third-party apps. This comparison helps to clarify that device manufacturers may not have higher security and privacy standards than third-party organizations. On the other hand, nearly all respondents, including users and non-users,

have little privacy concerns or remain neutral if data is shared with doctors or physicians. The most likely cause of this circumstance is that doctors and their organizations are legally required to comply with the privacy practices established by HIPAA.

For the non-users among the respondents, the most common reason selected for not using the health tracking feature on their devices is that they have no health concern; thus, there is no need to track their health. Only a small number of non-users are deterred from using health trackers due to privacy concerns. This result may imply that people may overlook the potential privacy risks and still use a health tracking device if there is a need.

Another important aspect of this survey is to learn whether users understand how their data may be handled by reading the privacy policies of their service provider. The results shown in Figure 1 indicate that most of the respondents do not or rarely read the privacy policies by answering 1 or 2 to the question. Consequently, they may have valued the convenience and functions provided by the apps and services more than their data privacy. Such a conclusion is similar to a previous statement that people may use health trackers when there is a need regardless of the privacy issues involved.

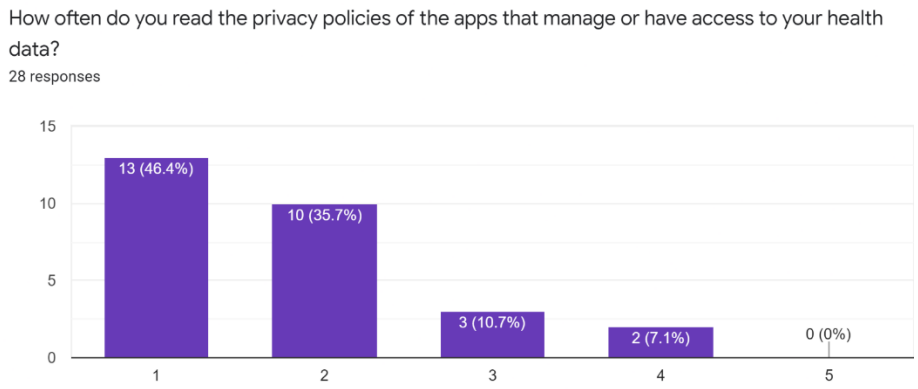


Figure 1. Survey Result Showing How Often Users Read Privacy Policies, 1 is never and 5 is always.

Lastly, as shown in Figure 2, when asked whether they believe that the government should regulate data privacy, most respondents answered yes (4 or 5) or remained neutral (3). Such a result shows that people may feel more secured with their data privacy when there are legal protections available, such as HIPAA.

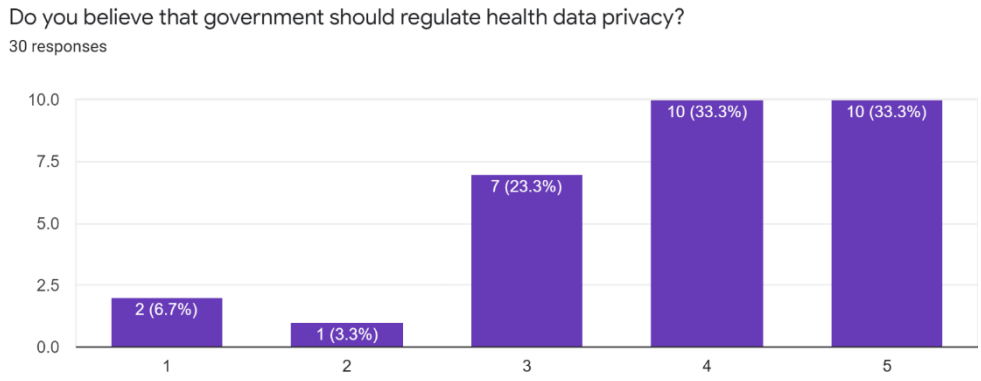


Figure 2. Survey Result Showing Users' Opinions About Government Regulations on Health Data Privacy, 1 is no or very negative, and 5 is yes or very positive.

The survey results indicate that many users and consumers have some concerns regarding the privacy of their health data. However, the results also reveal that most people do not read the privacy policies of their service providers, which creates a contradiction to the prior statement. Most users rely on the government to regulate and secure consumers' privacy rights, but the current regulations cannot provide sufficient protection. Companies may take advantage of this situation and use the health data collected in their best interests.

Healthcare Organizations

Health professionals and organizations are also relevant social groups in this study. Unlike technologies and businesses, healthcare providers are entities covered by HIPAA; thus, their practice must strictly comply with the standards created by HIPAA (Health Insurance

Portability and Accountability Act of 1996 (HIPAA) | CDC, 2018). In nearly all cases, these organizations can be trusted for protecting patients' privacy. An interview with a pediatrician has shown that healthcare organizations also utilize health data collected from patients' smartphones or wearables as there are certain benefits to use these data, such as higher accessibility. However, the transfer and secure storage of this type of data is often handled by a third-party organization. The privacy of the patients' data should remain uncompromised as these organizations meet the criteria of business associates under HIPAA's rules. Patients' data cannot be shared with any other outside organizations unless explicitly consented to by the patients. As a result, patients should have very little concern with their data privacy related to a healthcare provider.

Conclusion

In this digital world, health-related personal information and data are becoming increasingly available, accessible, and identifiable. Consequently, data privacy and security face new technological and social challenges. With technological advancements and better analytical capabilities, health information can be inferred and extracted from other types of data, such as social media posts. Additionally, de-personalized data for research purposes can be re-identified, compromising the privacy of the users and patients. With these data analytical methodologies, health data cannot be clearly defined and sharing of anonymized information with other organizations may also become a privacy concern, thus, creating technical challenges for health data privacy protections.

Another aspect of privacy challenge is insufficient legal protections. The current federal law that protects patients' health privacy rights is HIPAA, which establishes a standard set of privacy practice guidelines that must be followed by healthcare providers, health insurance

companies, and their business associates. However, with the digitization of health data and services, an increasing quantity of health data is collected by organizations outside of HIPAA coverage, including technology companies like Apple, Facebook, and Fitbit. As a result, users' data privacy is only protected by each organization's policy, which may vary significantly in terms of strength. Although most users do not trust companies with their data privacy, they also do not read the privacy policy of their service providers according to the survey result. They will not a limited understanding of how their data may be managed and utilized and will be unaware of the risks involved when sharing their personal information. Such an act of irresponsibility will greatly compromise their data privacy.

Digital health tracking and management devices and platforms have reshaped the ways that people can receive professional healthcare. However, they have also redefined health data privacy. Traditionally, healthcare services are performed in private settings, and patients' health data are stored in secured, physical locations. With the new technologies, patients' health data can be accessed anywhere on the internet. While consumers have concerns about their privacy, many are relying on the government to protect their privacy rights. However, the legal protections provided by the government for health data privacy are limited. As a result, data privacy is often only regulated by the privacy policies created by companies. Thus, users have often voluntarily allowed the companies to control the access and usage of their data. Companies can potentially utilize any personal information collected as a profit-generating tool since there is not any federal regulation that would prevent such actions. As a result, digital health data collection and management technologies have commodified users.

To better ensure health data privacy, a collaborative effort from the users, businesses, and legislators is required. Users should act more responsibly with their data by understanding how

shared data may be utilized and evaluating the privacy risks involved. Companies and businesses should protect users' health information by employing technologies, such as end-to-end encryption, to ensure the security of these sensitive data. Legislators should improve privacy laws to better suit the current technologies. For example, one possible improvement may be expanding HIPAA's list of covered entities to incorporate business organizations and enhancing users' ability to manage their data, such as requesting deletion of their shared data. The California Consumer Privacy Act provides an appropriate framework for new federal privacy legislation. These suggestions can help to encounter privacy challenges created by current technologies. However, as technologies continue to evolve, new issues will emerge, and more comprehensive legal protections and security protocols and procedures will be required.

Bibliography

Apple.com. 2020. *Legal - Apple Privacy Policy - Apple*. [online] Available at: <https://www.apple.com/legal/privacy/en-ww/> [Accessed 9 April 2021].

Apple Support. 2019. *About the privacy and security of your health records*. [online] Available at: <https://support.apple.com/en-us/HT209519> [Accessed 9 April 2021].

Al Ameen, M., Liu, J. and Kwak, K., 2010. Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications. Journal of Medical Systems, 36(1), pp.93-101.

Bari, L. and P. O'Neill, D., 2019. Rethinking Patient Data Privacy In The Era Of Digital Health. *HEALTH AFFAIRS BLOG*, [online] Available at: <https://www.healthaffairs.org/do/10.1377/hblog20191210.216658/full/> [Accessed 8 April 2021].

Cdc.gov. 2018. *Health Insurance Portability and Accountability Act of 1996 (HIPAA) | CDC*. [online] Available at: <https://www.cdc.gov/phlp/publications/topic/hipaa.html> [Accessed 29 April 2021].

Chancellor, S., Birnbaum, M., Caine, E., Silenzio, V. and De Choudhury, M., 2019. A Taxonomy of Ethical Tensions in Inferring Mental Health States from Social Media.

Proceedings of the Conference on Fairness, Accountability, and Transparency - FAT* '19,.

Ching, K. and Singh, M., 2016. Wearable Technology Devices Security and Privacy Vulnerability Analysis. International Journal of Network Security & Its Applications, 8(3), pp.19-30.

Dean, S., 2020. It's 2020 And You Have New Privacy Rights Online. But You Might Have To Show ID. [online] Los Angeles Times. Available at: <https://www.latimes.com/business/technology/story/2020-01-01/ccpa-california-internet-rights-what-you-need-know> [Accessed 8 November 2020].

Fitbit.com. 2020. *Fitbit Legal Privacy Policy*. [online] Available at: <https://www.fitbit.com/global/us/legal/privacy-policy> [Accessed 9 April 2021].

Goggin, B. (2019, January 06). Inside Facebook's suicide algorithm: Here's how the company uses artificial intelligence to predict your mental state from your posts. Retrieved December 03, 2020, from https://www.businessinsider.com/facebook-is-using-ai-to-try-to-predict-if-youre-suicidal-2018-12?op=1

Gostin, L., Halabi, S. and Wilson, K., 2018. Health Data and Privacy in the Digital Era. JAMA, 320(3), p.233.

HHS.gov. 2017. *HITECH Act Enforcement Interim Final Rule*. [online] Available at: <https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html> [Accessed 29 April 2021].

Lubarsky, B., 2017. RE-IDENTIFICATION OF “ANONYMIZED DATA”. *GEO. L. TECH. REV.*, pp.202-212.

McDermott, Y., 2017. Conceptualizing the right to data protection in an era of Big Data. Big Data & Society, 4(1), p.205395171668699.

Motti, V. and Caine, K., 2015. Users' Privacy Concerns About Wearables. Financial Cryptography and Data Security, pp.231-244.

Newman, D. (2019, May 03). What Is Privacy In The Age Of Digital Transformation? Retrieved December 03, 2020, from https://www.forbes.com/sites/danielnewman/2019/05/02/what-is-privacy-in-the-age-of-digital-transformation/?sh=246b3e96628e

Obar, J., 2015. Big Data andThe Phantom Public: Walter Lippmann and the fallacy of data privacy self-management. Big Data & Society, 2(2), p.205395171560887.

Ostherr, K., Borodina, S., Bracken, R., Lotterman, C., Storer, E. and Williams, B., 2017. Trust and privacy in the context of user-generated health data. Big Data & Society, 4(1), p.205395171770467.

Paul, G. and Irvine, J., 2014. Privacy Implications of Wearable Health Devices. Proceedings of the 7th International Conference on Security of Information and Networks - SIN '14,.

Raij, A., Ghosh, A., Kumar, S. and Srivastava, M., 2011. Privacy risks emerging from the adoption of innocuous wearable sensors in the mobile environment. Proceedings of the 2011 annual conference on Human factors in computing systems - CHI '11,.

Rippy, S., 2021. *US State Comprehensive Privacy Law Comparison*. [online] Iapp.org. Available at: <https://iapp.org/resources/article/state-comparison-table/> [Accessed 9 April 2021].

Sleep Cycle alarm clock. 2018. *Privacy Policy - Sleep Cycle alarm clock*. [online] Available at: <https://www.sleepcycle.com/privacy-policy/> [Accessed 9 April 2021].

State of California - Department of Justice - Office of the Attorney General. n.d. *California Consumer Privacy Act (CCPA)*. [online] Available at: <https://www.oag.ca.gov/privacy/ccpa> [Accessed 9 April 2021].

TRUSTe National Cyber Security Alliance U.S. Consumer Privacy Index 2016 Infographic [PDF]. (2016). TRUSTe, Inc.

Van Dijck, J. and Poell, T., 2016. Understanding the promises and premises of online health platforms. Big Data & Society, 3(1), p.205395171665417.

Vezyridis, P. and Timmons, S., 2017. Understanding the care.data conundrum: New information flows for economic growth. Big Data & Society, 4(1), p.205395171668849.

Zhou, W. and Piramuthu, S., 2014. Security/privacy of wearable fitness tracking IoT devices. 2014 9th Iberian Conference on Information Systems and Technologies (CISTI),.

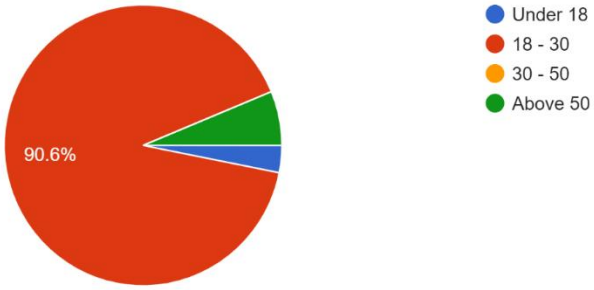
Appendix A: Health Data Privacy Survey Questions

1. What is your age?
2. Please specify your sex:
3. Do you use a device, such as a smartphone or a smartwatch, to track your health regularly?
4. If yes, please select your reason(s) for using the health tracking feature on your device?
5. Do you trust the device manufacturers to protect the privacy of your health data?
6. Do you share any of your data with third-party apps?
7. Do you worry about your privacy when sharing health data with third-party apps?
8. Do you share any of your data with doctors or physicians?
9. Do you worry about your privacy when sharing health data with doctors?
10. How often do you read the privacy policies of the apps that manage or have access to your health data?
11. Do you believe that government should regulate health data privacy?
12. If you do not use a device to track your health, what is your main reason for not using this feature?

Appendix B: Health Data Privacy Survey Result. Answer 1 means no or very negative, and answer 5 means yes or very positive.

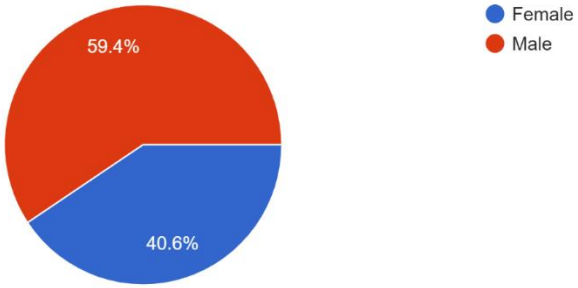
What is your age?

32 responses



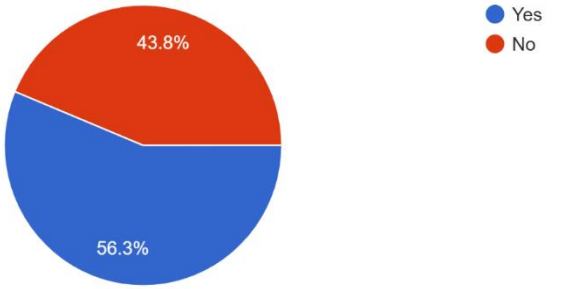
Please specify your sex

32 responses



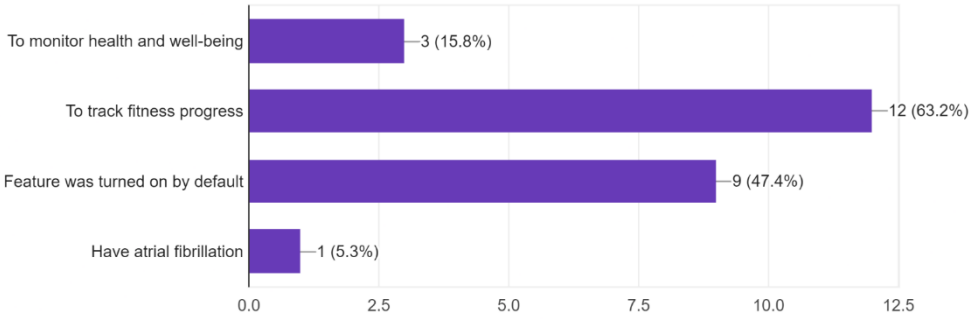
Do you use a device, such as a smartphone or a smartwatch, to track your health regularly?

32 responses



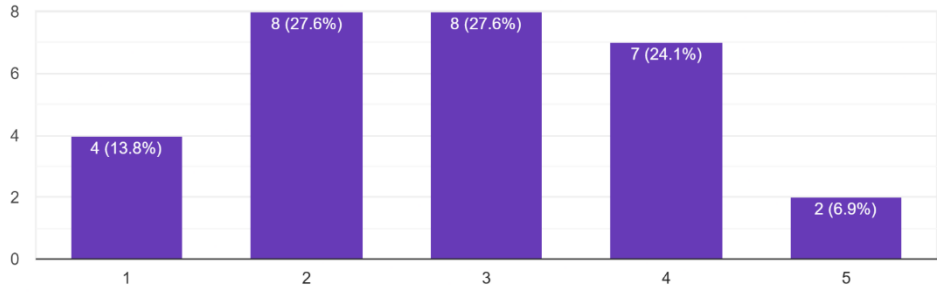
If yes, please select your reason(s) for using the health tracking feature on your device?

19 responses



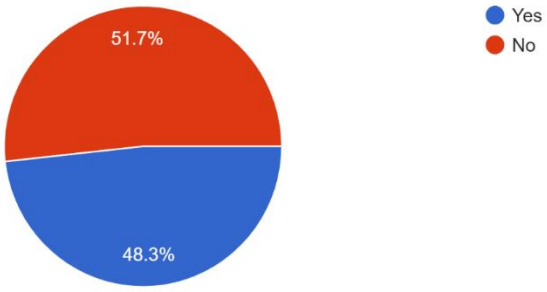
Do you trust the device manufacturers to protect the privacy of your health data?

29 responses



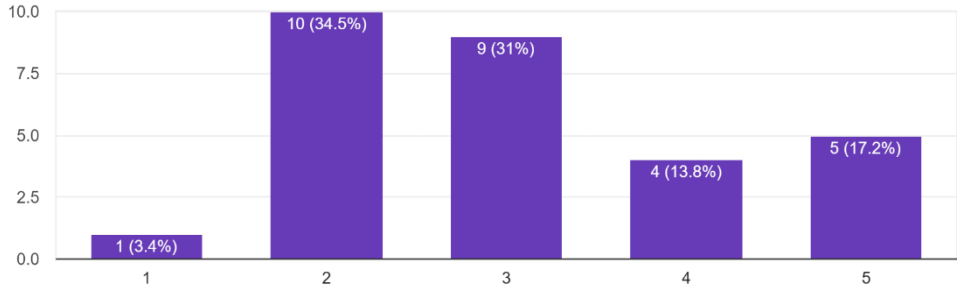
Do you share any of your data with third-party apps?

29 responses



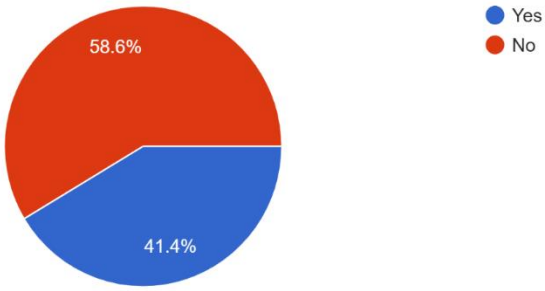
Do you worry about your privacy when sharing health data with third-party apps?

29 responses



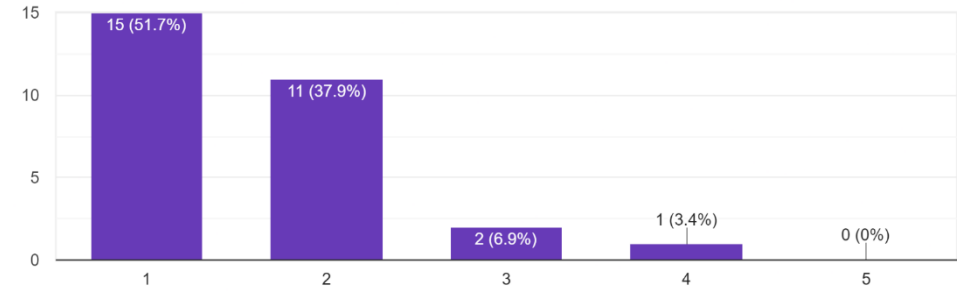
Do you share any of your data with doctors or physicians?

29 responses



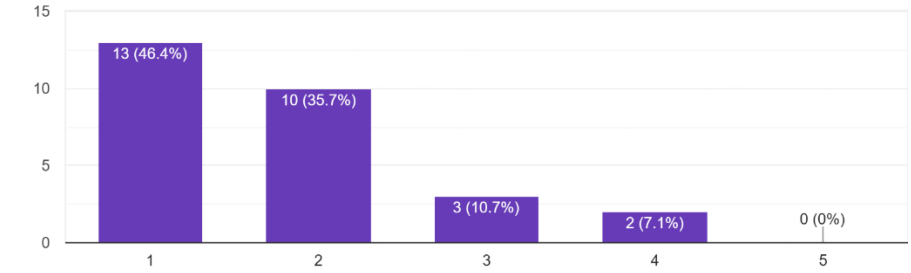
Do you worry about your privacy when sharing health data with doctors?

29 responses



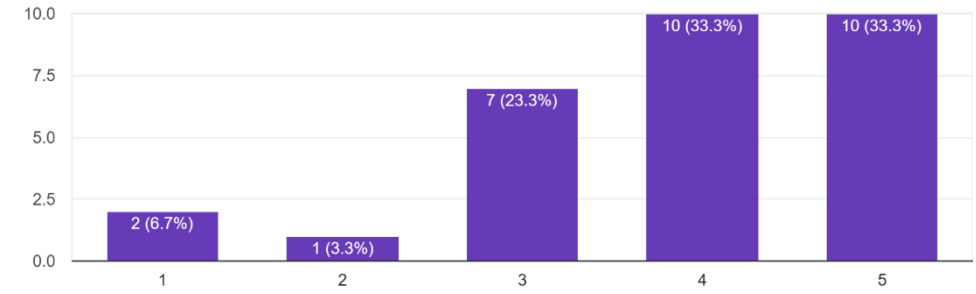
How often do you read the privacy policies of the apps that manage or have access to your health data?

28 responses



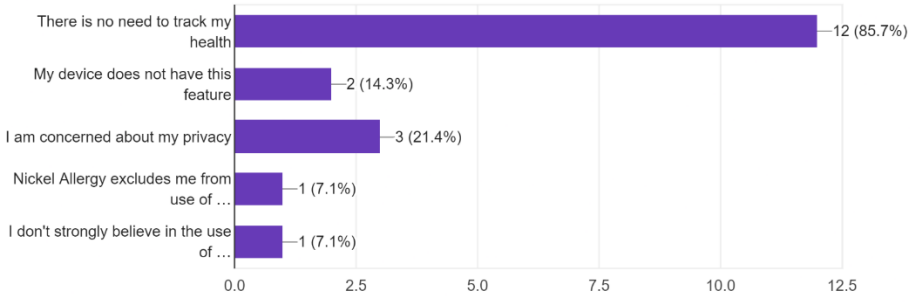
Do you believe that government should regulate health data privacy?

30 responses



If you do not use a device to track your health, please select your reason(s) for not using this feature?

14 responses



Appendix C: Interview Questions for Health professionals

1. Are you an out-patient or in-paitent physician?
2. Please specify your specialty
3. Does your organization utilize health data collected from smartphones or wearable devices?
    a. Yes:
        i. What methods does your organization utilize to transfer the data from patients' devices to your system?
        ii. What technology does your organization use to secure patients' digital health data?
        iii. What are the benefits of using health data collected from users' devices?
    b. No:
        i. What is the main reason that your organization does not use this data? Privacy concerns or others?
        ii. Does your organization have any future plans to start using digital health data as technology improves?
        iii. Does your organization store any medical data electronically? If yes, please specify the technology utilized to secure patients' privacy.
4. Are there any circumstances when patient health data will be shared with outside organizations (including other healthcare systems, research facilities, and businesses)?
    a. Yes:
        i. Are these organizations obligated to protect patients' privacy?
        ii. What technology is utilized to secure the transfers of the data?

iii. Do patient consents always need to be given in these circumstances?