Assessing Implications of Telehealth Apps' Privacy Policies and Terms of service for Users

Arpita Saxena

School of Information, University of Michigan

Master's Thesis Option Program (MTOP)

Dr. Casey Pierce

April 30, 2022

Introduction

In the modern era, HIPAA (Health Insurance Portability and Accountability Act, 1996) establishes high standards for the privacy and security of health information (Anthony et al., 2014) and remains the most critical law related to healthcare privacy because it provided a direct and unavoidable right to privacy for all patients. (Goldstein & Pewen, 2013; Majumdar & Guerrini, 2016; Cohen & Mello, 2018). Yet, significant challenges remain (Furstenburg, 2020) among the individuals concerning the vulnerability of their health data due to the presence of digital health tools. (Theodos & Sittig, 2020).

To scrutinize further, only the 'covered entities' (Vanderpool, 2019) are required to comply with HIPAA which includes health plans (Cauchi, 2011), health care providers, health care clearinnghouses. (Office for Civil Rights, 2013)

In addition, business associates are also bound by HIPAA. It involves a person or organization, other than a member of a covered entity's workforce. (Office for Civil Rights, 2013, p 3) It means that covered entities and other parties enter into a contract that ensures that the protected health information (PHI) of the users will be safeguard, it is known as business associate agreement (BAA). (Bassan, 2020)

HIPAA does not cover data created or held by a person or company that is not a covered entity or business associate. The de-identification of data by HIPAA places no limit on the use or disclosure. (Center for Democracy & Technology, 2020)

Amidst the Covid-19 pandemic and restrictions impacting physical activity and mental wellness (Radtke et al., 2021), telehealth use and its adoption in the United States increased to provide virtual health care services to individuals regardless of their ethnicity and racial differences along with electronic information online. (Park et al., 2018; FAIR, 2019; Fischer et

al., 2020, Castillo & Anthony, 2021) The “Health Resources and Services Administration (HRSA) of the U.S. Department of Health and Human Services defines it as the use of electronic information and telecommunications technologies to support and promote long-distance clinical health care, patient and professional health-related education, public health, and health administration.” (Telemedicine and Telehealth, 2020, p 1)

Some of the telehealth platforms are Direct-to-Consumer (DTC) telehealth. It is distinct from other telehealth because the patient initiates the care here. (Mehrotra et al., 2018; Jain & Mehrotra, 2020). They are more likely to be provided in the patient’s home. Patients can select any DTC telehealth platform on these websites or applications as per the requirement. According to their clinical issue, they can select a clinician and submit the request.

All telehealth platforms (DTC or not) come under HIPAA compliance. However, telehealth providers have been very challenging to abide by HIPAA audit protocol (Zhou et al., 2019) to get telehealth technology partners willing to sign the Business Associate Agreement (BAA) to perform a security and privacy self-assessment on their telehealth systems and practice. (Shachar et al., 2018; Zhou et al., 2019) To go even further, HHS issued a notification of enforcement discretion regarding remote communication applications, software, and technology in March 2020. (Office for Civil Rights, 2020) It included video chat and communication platforms supporting telehealth visits, such as FaceTime, that did not require a BAA from these third-party vendors, as is generally required under HIPAA. (Theodos & Sittig, 2020) It allows clinicians and health care entities to use platforms that are not HIPAA compliant, such as Facetime and other commonly used channels. (Shachar et al., 2018)

Amongst all these information and regulations, information privacy (Julia et al., 2005) is acknowledged as an important issue as the privacy concerns in the users (Nass et al., 2009) who

are using telehealth services in the name of good faith are escalating. Moreover, it has come to the attention that privacy policy and terms of service documents which are recognized as the legal agreement describing the organization's practices on data collection, use, and disclosure of the consumer information (Julia et al., 2005) are criticized as being too feeble, or convoluted. Kasanoff et al.; Anton et al. (2001; 2003, as cited in Julia et al., 2005)

Literature Review

Regardless of the Covid-19, telehealth has always made care more convenient for the patients. (Ashwood et al., 2017; Kichloo et al., 2020) As the healthcare practices transitioned to the internet, as in the case of telehealth, where all the information is electronically communicated, the situation to protect the privacy and security of health information is getting complex every day. (Watzlaf et al., 2017)

Similarly, a review of the literature on the subject reveals that health care applications refer to themselves as wellness tools in their "privacy policies or terms and conditions in an attempt to circumvent legislation that mandates privacy protections for user data, such as the Health Insurance Portability and Accountability Act." Glenn (2014, as cited in Huckvale, 2019, p 2) The privacy policies are supposed to make users aware of how a company provides a safeguard to their data and how it is managed and shared. (Schaub et al., 2015; Huckvale et al., 2019) Information about data practices is a critical component of data protection frameworks and regulations worldwide. Greenleaf (2014, as cited in Schaub, 2015)

The need to provide clear and thorough privacy notices is essential as the users of these healthcare applications or websites trust them that their personal or medical information will be handled carefully and appropriately. (Huckvale et al., 2015) Furthermore, the ex-chairwoman of the Federal Trade Commission (FTC) said that "Consumers know, for instance, that a smart

thermostat is gathering information about their heating habits and that a fitness band is collecting data about their physical activity. But would they expect this information to be shared with data brokers or marketing firms? Probably not.” Ramirez (2015, as cited in Schaub, 2015, p 4)

Unfortunately, the failure to help users to make an informed decision in the existing privacy notices (Schaub et al., 2015; Huckvale et al., 2019) is not surprising. They are often lengthy, tedious, and vague in providing complete information on the use of collected data. Schawrtz (2009, as cited in Schaub, 2015)

It decreases the motivation to go through a privacy policy or terms of service documents or ignorance into reading one. It is backed up by some figures, like 91 percent of consumers simply accept legal terms and conditions without reading them. This figure rises to 97 percent when looking at consumers aged 18 to 34. (2017 Global Mobile Consumer Survey: US edition, 2017) According to another study, 36% of Americans never read a company's privacy policy before agreeing to it (Auxier et al., 2019)

The vast majority of users feel insecure about their personal/medical information on online platforms and agree that they rarely read privacy policies documents (McDonald & Cranor, 2008), and even if they do, they don’t understand them before deciding to use applications (McDonald & Cranor, 2008; Schaub et al., 2015).

With the availability of fuzzy privacy policies and the constant presence of healthcare data breaches (Seh et al., 2020), thirteen percent of respondents said they had ever withheld information from a provider due to privacy/security concerns. (Castillo & Anthony, 2015)

To encourage and motivate users to go through the privacy policy and terms of services documents, the paper aimed to provide a comprehensive assessment of some DTC telehealth

platforms' privacy policy and terms of service documents. As refined privacy policy and terms of service documents will also help some patients (of depression or mental health disorder) with privacy concerns to mitigate the risk of social devaluation. (Castillo et al., 2016)

The reason for selecting DTC telehealth platforms in this paper is that the patients commence the care here. The difference in the coordination of care from other health systems raises concerns as for-profit companies dominate it. Bodenheimer (2008, as cited in Mehrotra et al., 2018)

RQ1: How do telehealth applications communicate with users through privacy policy documents?

RQ2: How do telehealth applications communicate with users through their terms of service documents?

Materials and Methods

Study Design

The process of conducting a thorough analysis of the telehealth (TH) apps' documents starts by finalizing with a Descriptive study design. The purpose of selecting descriptive studies is to analyze the events or conditions by studying them as they are in nature without manipulating any of the variables. (Siedlecki, 2020)

Data Collection

The data collection process starts in May/June 2021. In the selection process of telehealth platforms, some of the inclusion criteria were identified as, firstly, authenticity of TH apps, which involves the extent to which an online platform is genuine. Dunne (2016; as cited in Morgan, 2022), secondly, provides online services in the US and lastly, which ranks among the top 20. With convenience sampling in focus, a total number of 14 telehealth platforms were

recognized and segregated according to their services - Mental health and general medical care (Table 1). With paucity of research on the topic, the reason of considering different type of platforms is to provide wide range of viewpoints on these apps. After deciding on 14 TH apps, their privacy policy and terms of service documents (makes upto 28 documents) were downloaded in pdf format.

Table 1

14 Telehealth Platforms

Services Provided	Mental Health Care	General Medical Care (including mental health)
	1. 7 cups 2. BetterHelp 3. Brightside 4. Talkspace	1. 98Point6 2. Amwell 3. BCBSM 4. Doctor on Demand 5. K Health* 6. Lemonaid 7. LiveHealth Online 8. MD Live 9. Plushcare 10. Teladoc

K Health* - AI Driven Digital Health (Perlman, 2020)

Data Analysis

For data analysis, I used NVivo software (release 1.5). The prime goal of qualitative analysis is to acknowledge a better in-depth understanding of the documents through first-hand experience and to make truthful reporting of the themes formed in the process of analysis. In addition, qualitative research are useful in dealing with diverse groups. (Cohen et. al, 2001, p.1)

Overall, I uploaded all 28 pdf documents to the software and read it multiple times to get familiarized with them. For the initial coding, individual documents were assessed to form initial themes to refine the data. Afterwards, common patterns were identified across atleast more than

3 documents. In the end, I formed 7 significant themes and their sub-themes to provide a detailed viewpoint on some statements in the documents regardless of the difference in the type of telehealth platforms. Operational definitions of the 7 major themes are as follows:

1. Healthcare Provider - The statements that give healthcare providers presence on the platforms and what rights they have.
2. Technology - The statements provide the technological limitations of the platforms.
3. Data - The statements elaborate on how the users' data is transferred or shared.
4. Users' rights - The statements that discuss the users' rights on the platform while availing of the services.
5. Confusing - The statements which are difficult to understand for the users.
6. Contradictory - The statements which give complete opposite meaning to the information.
7. Platform rights - The statements discuss the rights of the platforms.

Results

In the results section, all the themes and sub-themes are presented in figure format to visualize better. For this step, I created an excel sheet where all the themes and their sub-themes are addressed. Along with if any platform acts according to the sub-theme or not, and which does not mention anything. (Appendix 1)

I created one bar plot for every theme except for the Users' right theme, which is divided into two bar plots. One is an overview of the general rights of every user, and the second is focused on only California residents because, in 2018, the state of California passed a unique privacy law focused on protecting data privacy rights (Stephens, 2019) creating a sense of

injustice (described below). The bar plots were created with the help of RStudio software (ggplot2 package). Each plot has three legends in the figures - 'Yes,' 'No,' and 'Didn't mention'. The legend 'Yes' means acting following the sub-theme, 'No' nullifies the sub-theme, and 'Didn't mention' means it does not represent the sub-theme. Y-axis represents the number of counts of TH apps; the x-axis represents the sub-theme.

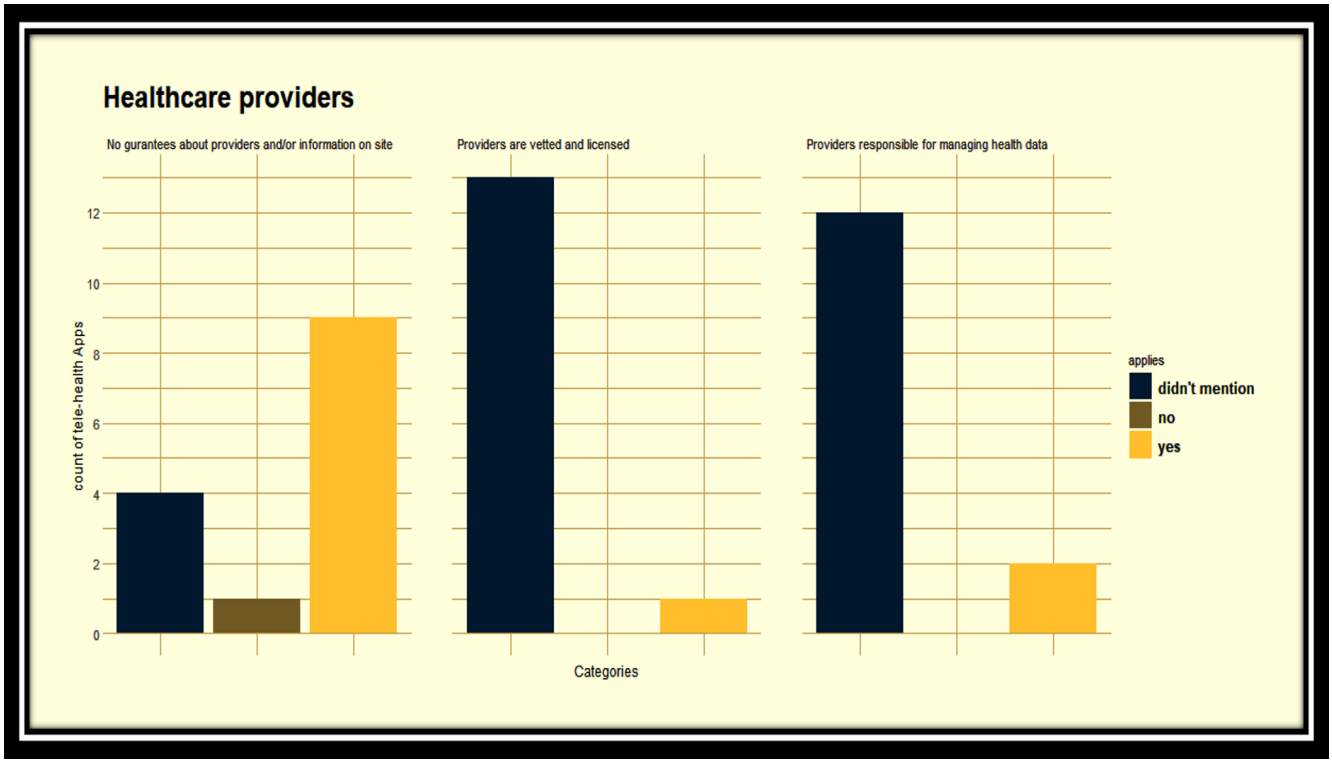
All the statements considered in the study are mentioned in Appendix 2.

Theme 1: Healthcare Providers

The category identifies the presence of healthcare providers on the platforms. It appeals as one of the biggest concerns as healthcare providers can provide telehealth services but will never be subjected to penalties for violation of privacy or security of personal health information. Moreover, it's users' responsibility to verify healthcare providers' credentials before even considering them, and if they do not do so, the platforms hold no liability for it. Furthermore, the theme is divided into three sub-themes (Figure 1).

"Amwell does not make any representations or warranties about the training or skill of any Providers using the Services. You are ultimately responsible for choosing your particular Provider on the Services." (Amwell Terms of Service, p 1)

Figure 1



Under **'No guarantee about providers and/or information on site,'** in which 9 TH apps stated their disagreement in providing any authorization of healthcare providers working on their platforms. Of the remaining five apps, four apps did not mention anything, and just one app confirms this crucial information of providers. The findings are delicately expressing that the information available on the platforms is just for educational purposes and should not be taken seriously. The advice provided by the professionals is not liable as the platforms do not have any credentials on them.

Under **'Providers responsible for managing health information'**, 12 apps did not mention this critical information in their documents. Only two apps explicitly state that it's the providers' responsibility to manage users' health information.

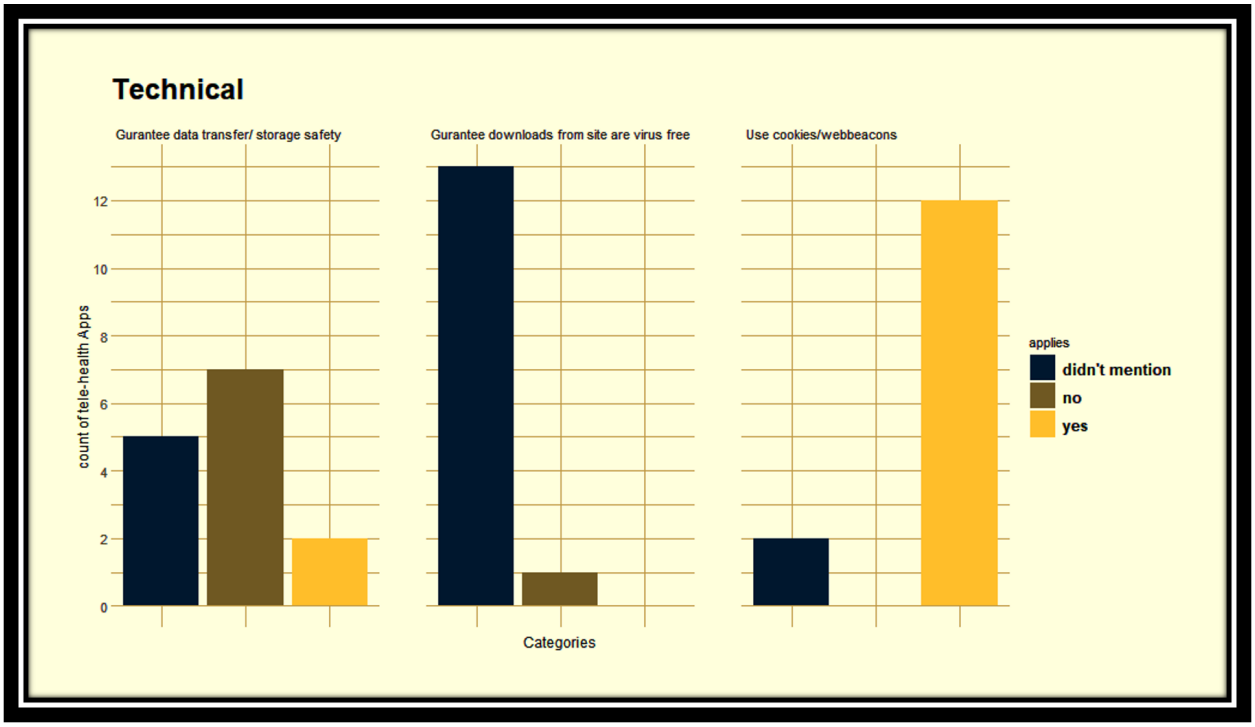
Under **'Providers are vetted and licensed,'** only one app provides this comforting information in their documents where users need not worry about having quality and reliable therapy sessions. Rest of the telehealth platforms do not mention anything about the licensure of the healthcare providers working on the platforms. It can create a wave of chaos between the users if they find out about this misleading information.

Theme 2: Technical

The theme elaborated on the technical aspect of the documents and how it has out-spaced users' privacy protections. It is straightforward for telehealth companies to easily access information that threatens privacy and control users' health information through these platforms. As given in Figure 2, there are three sub-themes represented.

"Lemonaid Health cannot and does not guarantee or warrant that email or files available for downloading from its Site will be free of viruses or other code that may contaminate or destroy data on your computer. You are responsible for implementing sufficient protective procedures and checks to maintain the accuracy of your data for maintaining a data back-up or other means for the reconstruction of any lost data." (Lemonaid Terms of Service, p 8)

Figure 2



Under **'Guarantee data transfer/storage safety,'** only 2 TH platforms provide their affirmation in protecting users' data in terms of store and transfer, and 7 TH platforms give their disagreement in doing so. Five do not mention anything about it. The key findings were opaque, especially in the domain of health information, when the population is vulnerable and trying to seek mental health therapy because they might not prioritize their private and sensitive data. The statements mention that they don't guarantee to store the data safely, making it easily hackable. Moreover, the platforms that don't claim anything are more dangerous because they have a loophole to defend themselves if anything goes wrong with the users' data.

Under **the 'Guarantee downloads from sites is a virus-free** sub-category, no app mentions their support in providing virus-free information on their websites and does not consider the importance of this feature. Itt leads to the point that it is hard to trust these platforms

as they don't have any up-to-date anti-virus protection. It is not just about gaming the risk on health information data but also about personal devices like computers and laptops. mobiles etc.

Under **'Use Cookies/ Web Beacons,'** 12 TH apps indicate this as a positive statement where they use cookies or web beacons to share information with third parties. Users have the full right to disable the cookies if they don't want their data to be tracked.

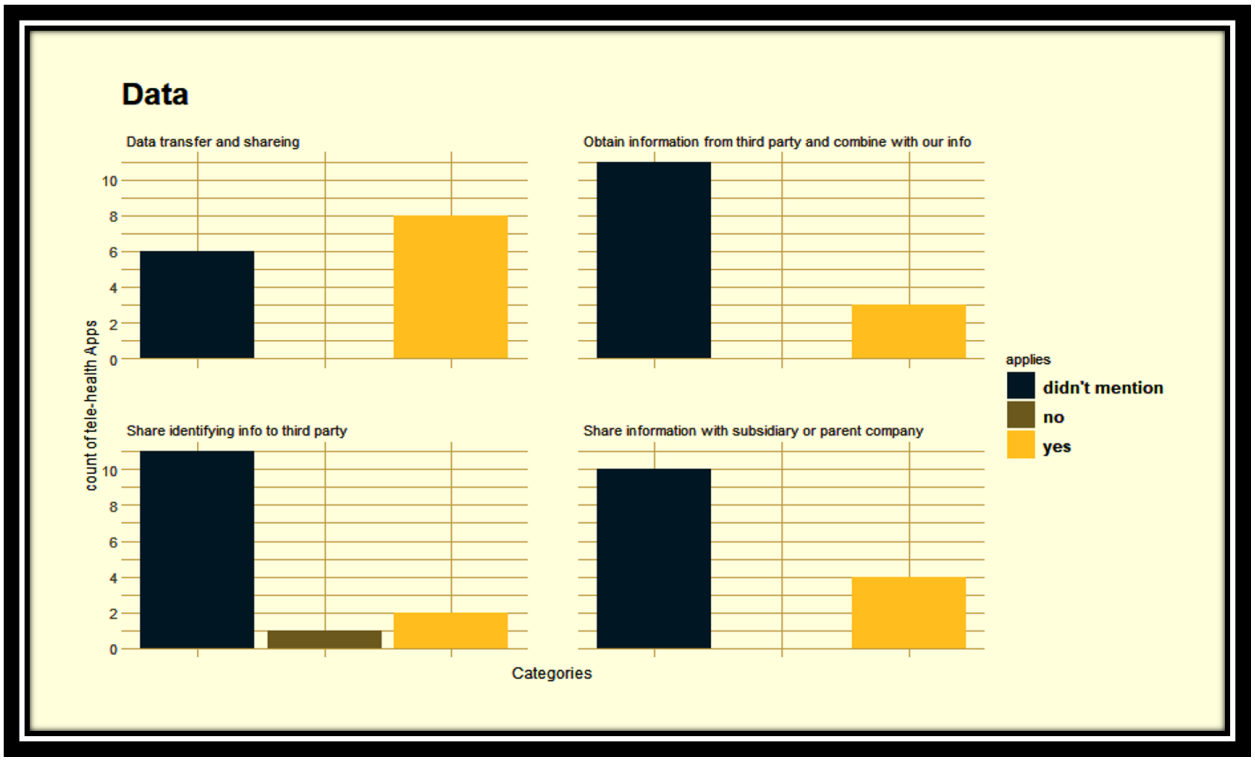
Theme 3: Data

The theme is focused on how privacy policy documents of TH apps do not clarify what kind of data can be shared and in what situation it can be used by other companies freely without any notice to the users. Figure 3 summarizes the sub-themes of 'Data'.

"Through our Services, we may allow third party advertising partners to set Technologies and other tracking tools to collect information regarding your activities and your device (e.g., your IP address, mobile identifiers, page(s) visited, location, time of day). We may also combine and share such information and other information (such as demographic information and past purchase history) with third party advertising partners. These advertising partners may use this information (and similar information collected from other websites) for purposes of delivering targeted advertisements to you when you visit third party websites within their networks."

(Brightside Privacy Policy, p 5)

Figure 3



Under **'Data Transfer and sharing,'** 8 apps affirms that they can transfer or share the users' data in case of acquisition and bankruptcy. Six apps do not mention how they will use the data in unforeseen situations. As users use the platforms and provide the data, their health information might not be treated as confidential.

Under **'Obtain information from the third party and combining with users' info,'** three apps say they can combine users' information with third-party advertising partners. And 11 apps did not mention it in their documents.' The statements mention that they may expose users' data to third parties for advertising or marketing purposes.

Under **'Share identifying info to third-parties,'** two apps share users' information with third parties for promoting medical and clinical research. Only one app declined, and 11 apps did

not mention it. From a users' perspective, this can be an unacceptable approach by telehealth platforms to use users' information for their benefits.

Under **'Sharing information with subsidiary or parent company,'** 4 TH apps provide users' information to their parent or subsidiary companies with their consent or knowledge. Eight apps did not offer any understanding of it in their documents. It provides a lot of gray areas in the privacy policy and terms of use documents. Users can't understand the context behind it and unknowingly feed information to other companies he is not even a part of; documents like this are built to constantly exchange user data with other parties, who use that data for their purposes like marketing or advertising.

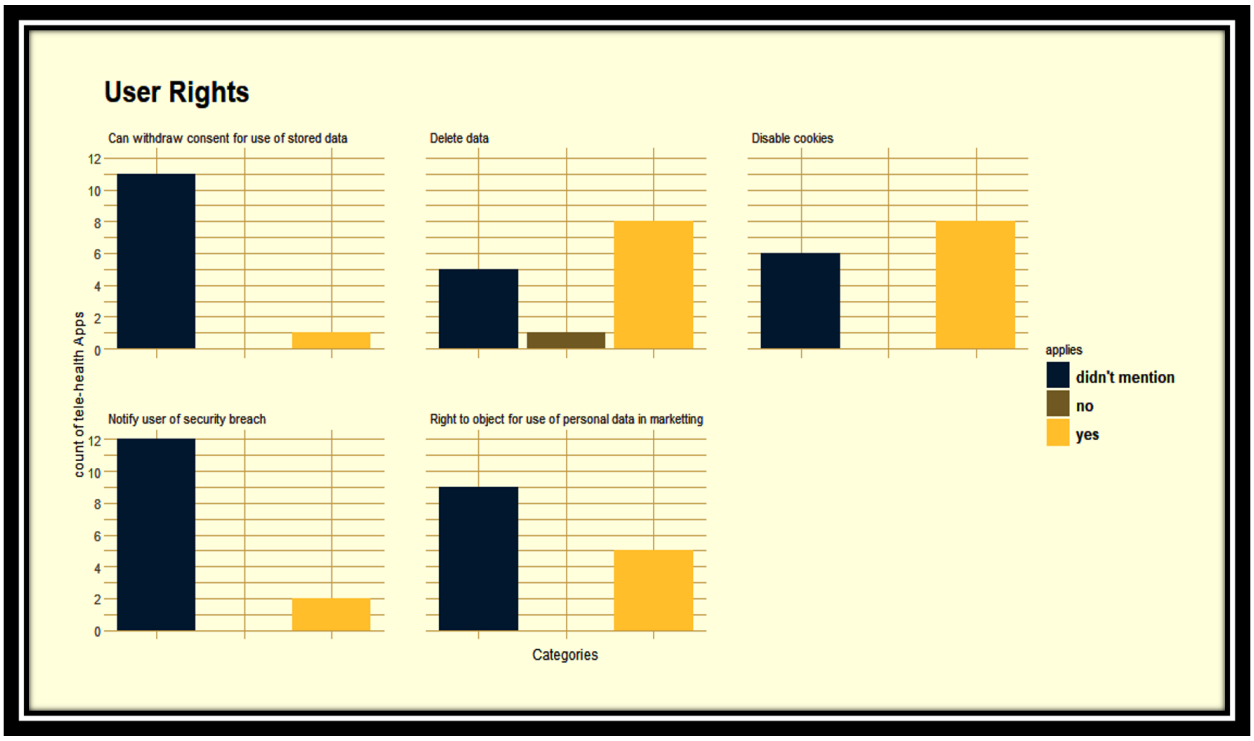
Theme 4: Users' rights 1

The theme focuses on that users get rights concerning their information and how the app will use it. It is sub-categorized into areas where users can control their data in Figure 4.

"Subject to applicable law, you may withdraw your consent to uses and disclosures of Personal Information as outlined in this Privacy Policy. You must submit your request in writing to Teladoc. Withdrawing consent does not invalidate consent to any collection, use or disclosure of Personal Information to which you consented before consent was withdrawn. If you withdraw consent, or refuse further consent, Teladoc's ability to offer services to you may be limited."

(Teladoc Privacy policy, p 3)

Figure 4



Under **'Can withdraw consent for the use of stored data,'** only 1 TH app gives full disclosure that users' have every right to decide whether they want their personal information to be used by the platforms or not. Unfortunately, 13 apps did not mention this right and kept it in a gray area of their privacy policy.

Under **'Delete data,'** 8 TH apps allow users to delete their data in various forms; for instance, users' can suppress their data, or if the information is incorrect, users can request to delete their data. Interestingly, some apps have put conditions, like users' do not get the option to delete their data for research purposes, and the data has already been sold to third parties. They cannot remove their medical records, or the platform has the right to store the data for seven years under the law and only allows deletion of public posted user data. Only one app does not allow the users to delete their data.

Under **'Disable cookies,'** 8 apps allow users to disable cookies with some constraints like if cookies are disabled, the site will not work correctly, or the flash cookies will be re-created afterward. The users can only delete google analytics cookies to hide their interaction with website content. Six apps did not mention users' control over cookies in their documents.

Under **'Notify user of a security breach,'** only two apps elaborated on this statement in their document. Twelve apps didn't mention anything about informing users of a security breach. This is a sensitive topic because if users are notified of any security breach, they get every right to claim compensation from an organization if they suffered damage due to it breaking data protection law. By not providing any detail on it, the platforms cannot offer anything to their users.

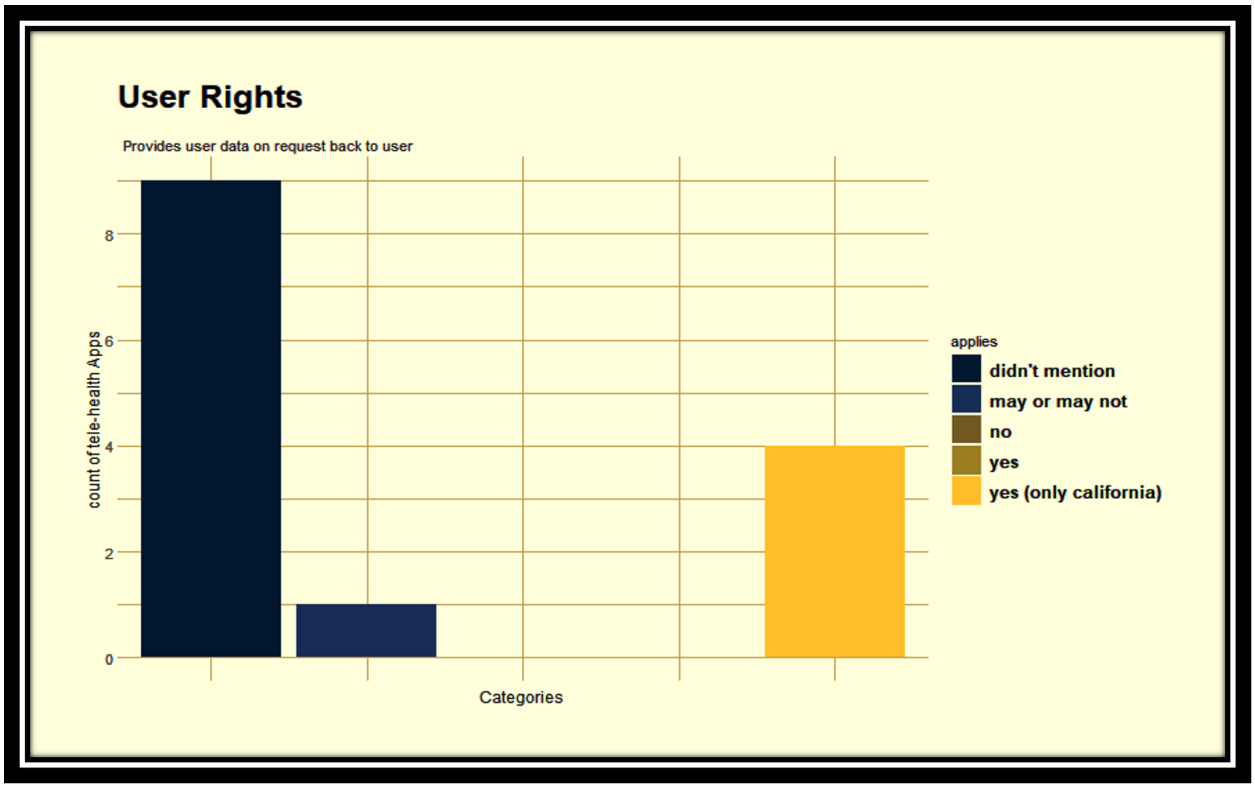
Under **'Right to object for the use of personal data in marketing,'** 4 apps respect users' privacy and allow them to object if their data is used for marketing purposes. This way, the platforms cannot use users' data to sell or promote things. Nine apps did not mention it, and it does not apply to one app.

Theme 4: Users' rights 2

The theme is focused on providing individual rights to California residents. (Figure5) It creates a sense of injustice among the community where different benefits are provided to people from California.

"California residents are entitled once a year, free of charge to request and obtain certain information regarding our disclosure, if any, of certain categories of personal information to third parties for their direct marketing purposes in the preceding calendar year. We do not share personal information with third parties for their own direct marketing purposes." (Amwell Privacy Policy, p 3)

Figure 5



Under **'Provides user data on request back to the user,'** this is a unique sub-category where four apps give the special right to only California residents that their data can be returned to them. One app provides an unclear instruction that they might not be able to return every time without elaborating on it.

Theme 5: Confusing

The theme is focused on confusing statements in the privacy policy documents. (Figure 6) It is an essential theme because when users with no medical background look at some medical terms, it gets hard to comprehend the document's information. Some statements mentioning medical research, marketing, or healthcare providers are blurred to get something out of them.

"You agree to indemnify and hold PlushCare, its subsidiaries, affiliates (including the Providers), officers, agents, and other partners and employees, harmless from any loss, liability, claim, or demand, including reasonable attorney's fees, made by any third party due to or arising out of (a) your use of the Websites or the Service in violation of this Agreement, (b) your failure to comply with applicable laws and regulations; and/or (c) your breach of this Agreement and/or any breach of your representations and warranties set forth above." (Plushcare Terms of Service, p 10)

Figure 6

Under **'Confusing corporate/service structure,'** 3 apps provide poor structure and incoherent sentences in their privacy policies, making it very difficult for users to grasp them. So, even if a user tries to go through the privacy policy or terms of service documents, it can be

hard to understand them. It can demotivate users to try further reading the documents in the future.

Under **'Need to sign doc for using service,'** to further elaborate on the sub-theme, of 14 TH apps, only one app asks its users to abide by every point on their documents. In the rest of the platforms, just the sign-in process automatically makes users comply with the documents.

Under **'Photos and videos uploaded become site IP without royalty,'** two apps make it confusing for the users to understand the context behind the statement in the era of photoshop. This indicates that if a user is uploading or sharing any photos or videos via the platform, the platform can use them anywhere for their benefit without taking consent from the user.

Under **'Use service at your own risk,'** 4 apps openly mention that they do not provide any protection to the users' health information data, and it is all at users' disposal if they want to take the risk of using the platform. It creates a highly complex situation for the vulnerable population trying to seek help from the telehealth platforms. It is hard for any user to trust a platform explicitly conveying that use it at your own risk.

Theme 6: Contradictory

The theme is focused on contradictory statements found in their privacy policy and terms of use documents. It was further divided into five sub-categories to provide a deep analysis of the area (Figure 7).

"You will indemnify us, defend us, and hold us harmless from and against any and all claims, losses, causes of action, demands, liabilities, costs or expenses (including, but not limited to, litigation and reasonable attorneys' fees and expenses) arising out of or relating to any of the following: (a) your access to or use of the Platform; (b) any actions made with your account or Account Access whether by you or by someone else; (c) your violation of any of the provisions of

this Agreement; (d) non-payment for any of the services (including Counselor Services) which were provided through the Platform; (e) your violation of any third party right, including, without limitation, any intellectual property right, publicity, confidentiality, property or privacy right. This clause shall survive expiration or termination of this Agreement." (BetterHelp Terms of Service, p 4)

Figure 7

Under **'Change privacy policy at any time'**, none of the apps mentions having the informed policy change criteria. And four apps explicitly give their affirmation for the same. The following statement captures both positive and negative context about updating the document. So even if a user tries to go through the documents before using the services on the platform, it is highly unacceptable to expect that the user would want to reread them by himself amidst the treatment. It is an essential point to focus on, and the platforms should inform the users before making any documents changes.

Under **'Hold harmless and indemnify us,'** 4 apps give conflicting statements for users about being responsible for actual losses and potential liabilities. In unforeseen situations, users can pay unnecessarily for an attorney or third-party fees. To further elaborate, if there is any dispute with the platform, the users have to protect the platform in any way possible.

Under **'No service to Medicare or Medicaid,'** it is very unprofessional of one TH app to mention this rule. It indicates unfair treatment towards seniors with Medicare or users with Medicaid who are likely to fall for general medical care cannot receive the services from the platform.

Under **'Provide personal info at your own risk,'** only two apps give this antithetical statement due to which users are at significant risk of identity theft, stalking, and harassment. In the previous theme of confusing, some of the platforms mentioned using the services at their own risk, and this theme says about providing the personal information at their own risk. So, even if the users have any right on the platforms, these statements automatically nullify every right a user can have on the platforms.

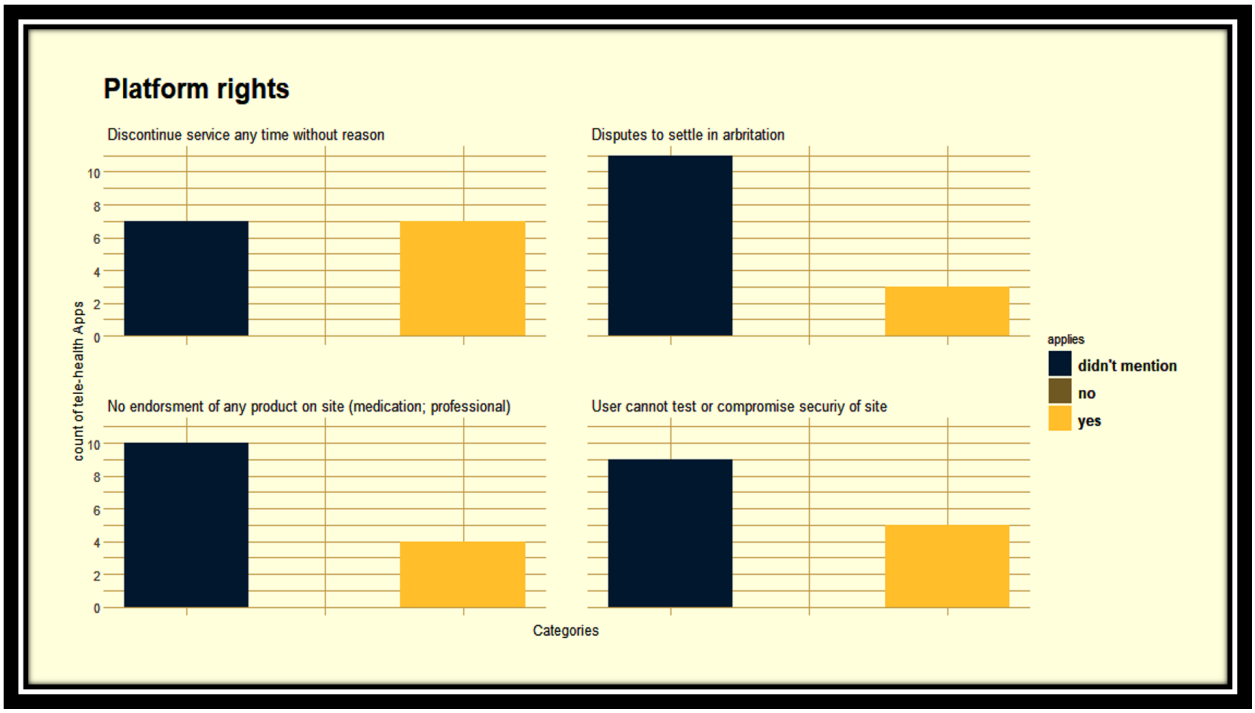
Under **'Take in-person care (even if the platform says otherwise)'**, 7 apps agree that they provide falsified information on their website page about educational articles on anxiety and depression through this sub-category. Overall, the contradictory statements of information or service include misleading presentations. It can easily be used to derive sensitive information.

Theme 7: Platform rights

The theme is focused on how the platforms will collect, use, and process data that they collect on behalf of their users. It is further sub-categorized into four parts in Figure 8. None of the apps negate any of the points described below; it is either an affirmation or does not mention.

"Any dispute or claim relating in any way to your use of the Talkspace Service will be resolved by binding confidential arbitration, rather than in court. The Federal Arbitration Act and federal arbitration law apply to these Terms. There is no judge or jury in arbitration, and court review of an arbitration award is limited. However, an arbitrator can award on an individual basis the same damages and relief as a court (including injunctive and declaratory relief or statutory damages) and must interpret these Terms as a court would." (Talkspace Terms of Service, p 9)

Figure 8



Under **'Cannot test or compromise the security of the site'**, five apps give very vague instructions to their users for doing almost everything on their website can result in a violation. Firstly, the platforms do not set a high standard for securing users' information, making it easily hackable, and secondly, they expect users to not modify or destroy anything on their platforms.

Under **'Discontinue service at any time without reason'**, seven apps can terminate or delete users' accounts without giving any prior notice or written reason to explain the cause of discontinuation. Amidst a treatment, a users' account can be deleted by the platform without providing any reason is ethically wrong.

Under **'disputes to settle in arbitration'**, three apps follow the negotiation process in case of any dispute or claim relating to their security. this does not give users an option to claim their rights legally. Under no circumstance, any user at harm (because of the platform) cannot sue them. Eleven apps did not provide any information on their document that how will any dispute be solved if it occurs.

Under **'No endorsement of any product on site (mediation or professional),'** 4 apps have mentioned in their document that they will not be liable for any services or recommendations given by healthcare providers who are working from the platforms or anything that is provided on the platform like prescriptions, educational videos or articles, etc.

Discussion

In the results section, the study talked about the privacy policy and terms of service documents of the selected telehealth platforms and how they control users' information. The findings suggest the availability of information is inconsistent and vague throughout the documents. It can be very inconvenient for the users to get a full grasp whose primary reason is to seek general medical care or mental therapy on the telehealth platforms, resulting in miscommunication between the users and platforms. It can be correlated with one of the studies that discuss the public's lack of understanding. (Auxier et al., 2019) It shows that 63% of Americans admit that they understand very little or nothing about the current laws and regulations to protect their data privacy. (Auxier et al., 2019) With patient's lack of trust in the

platform can significantly affect the quality of life. (Young et al., 2018) There is a need to apply basic ethical principles (Keenan et al., 2021) while using the virtual space to provide medical or mental care because of the lack of intimacy between the patients and the healthcare providers. Communicating the complete information properly with the users also helps to understand patients' preferences for using proper telehealth services in the future. (Predmore et al., 2021)

In the findings, some points focus on areas like the role of healthcare providers on the telehealth platforms and their rights to manage the users' information. In the analysis, some of the statements gave a surprising takeaway that the platforms hold no guarantee about the healthcare providers, and users should look out for their background check and credibility before agreeing to receive services. Moreover, healthcare providers have the right to manage users' health information. It all relies on good faith because, during the Covid-19 pandemic, the Office for Civil Rights (OCR) announced not to impose penalties on the covered healthcare providers for "noncompliance with the HIPAA rules." ((OCR), Notification of enforcement discretion for telehealth 2021, p 1)) This information can be uncomfortable for the users because of the increased concern for their privacy.

The availability of large chunks of data in the documents does not show high standards for protecting the information. The security protocols on the platforms are basic and represent that they can be easily hackable, encouraging a breach of data privacy. A report issued by U.S. Health and Human Services showed 686 healthcare data breaches in 2021, and 44,993,618 healthcare records have been exposed or stolen. (Largest Healthcare data breaches of 2021, 2021) The awareness of this particular point can discourage users from using telehealth platforms.

Understandably, platforms do not transmit data about a user without first obtaining the user's permission. However, in the findings, it is shown that some telehealth platforms do not even ask users to see or sign the privacy policy document. The just user login process permits platforms to use users' personal or medical information. The findings suggest that the platforms pose more like for-profit companies where they use users' data to form segmentation of heterogenous user groups based on their interests, beliefs, attitude, and opinions and use it for marketing purposes.

The lack of well-written privacy policy and terms-of-service documents are so incomprehensible. They lack a clear description of data collection practices. (Moretti & Naughton, 2014) They do not guarantee thoroughness. In the findings, all the selected platforms focus on mental therapy as either their sole service or in combination with general medical care and do not mention the security of the wellness or mental well-being of the users. In addition, the essential terms like consent do not show up in the documents, which suggests that users do not get much control over their data. Undoubtedly, users care greatly about their privacy, especially when using their personal or medical information. They should feel secure before using these telehealth platforms.

The study proposes some suggestions for the Policymakers and Regulators to make the patients' experience more smooth and comfortable on the telehealth platforms.

The study also considers some implications for HCI (Stephanidis (2001, as cited in Fetaji et al., 2007, pp 3-17)) to make these privacy policies and terms of service documents user-friendly with respect to user-interface design (UI). So that the users can easily access and understand them regardless of the system like smartphone, tablets, or computer/laptop they use.

Implication for Policymakers

The study proposed 'Consumer Privacy Framework for Health Data' to policymakers. The framework ensures the privacy of users' health data outside HIPAA protection. (Center for Democracy & Technology, 2020) It applies to DTC telehealth platforms because the communication between the patients and covered healthcare providers is virtual through many third-party communication channels like Zoom, FaceTime, etc. "No communications platform can be true HIPAA compliant as HIPAA compliance is about users, not technology." (Is FaceTime HIPAA compliant, 2022, p 2) Microscopically, if the healthcare data once fall under HIPAA protection (with a covered entity) does not mean that it will remain under the umbrella of HIPAA when it moves through unregulated platforms. (Center for Democracy & Technology, 2020)

As we discussed the presence of dense privacy policies in the results section, some of the main points of the framework are centered around limiting the amount of health information collection, disclosure, or what is required to provide the service/feature. The framework also favors restricting the sharing of information with third parties and the affirmative consent process. (Proposed Consumer Privacy Framework for Health Data, 2021) “The CDT/EHI framework would place collection, use, and disclosure limitations on health data and require that automated, algorithmic or artificial intelligence systems be designed and implemented to mitigate bias.” (McGraw & Mandl, 2021, p 2)

U.S. policymakers should actively consider this framework for DTC telehealth platforms. Also, should ask third parties to adopt the framework, leading to data sharing limitations ((McGraw & Mandl, 2021), and the users’ health information that transfers through unregulated online platforms or gets automatically shared with the subsidiary or parent companies will be protected.

Privacy policies should help reduce information asymmetries because companies share information with their customers. (McDonald & Cranor, 2008) Also, it is a favorable way to reinstall users' trust and avoid privacy and ethical issues to some extent and bring telehealth platforms to their full potential to provide healthcare services to the users.

Implication for Regulators

As mentioned in the findings, different comprehensive consumer privacy laws for other states, like California, can create a sense of injustice among users. Justice is one of the ethical principles most discussed concerning fairness and equal access to the rules concerning telehealth; it balances the needs of the individual with those of the wider community (Keenan et al., 2021). The findings and discussion of the study propose that during times like pandemics, it is appropriate to provide virtual care at its best and enhance the patient's experience to make it more accessible and convenient (Young et al., 2018). But in addition, it is also necessary to prioritize users' sentiments over their personal or medical information. More comprehensive standards and regulations may be needed to ensure strong privacy and security protections for telehealth and all electronic consumer information. (Hall & McGraw, 2014; McGraw & Mandl, 2021).

Implications for HCI

The re-designing of the privacy policy and terms of service documents is essential because users being the beneficiaries of the telehealth services, should receive a comprehensive understanding of the services and how their information will be collected, shared, and disclosed by the platform involved third parties.

The lengthy and overly complex documents (Schaub et al., 2015) should be made more user-friendly. Considering the delicacy of personal or medical information, it is important to

update them to be shorter and up-to-the-front to convey direct communication with the users. To sustain the information over time, graphical representations in the privacy policy documents might be useful for conveying data use practices to users. (Guo et al., 2020) The more basic approach by not including any complex medical terms or vocabulary can motivate and encourage the users to read and understand the privacy policy and terms of service documents.

Limitations

Some of the limitations found in the implementation of the study were the inclusion of only 14 DTC telehealth platforms due to time constraints. Secondly, the surveys or interviews to identify users' first-hand perceptions of the privacy policy and terms of service documents would have been a better fit for the findings and discussion.

Conclusion

The study's conclusion restates that it is essential for policymakers to re-design the policies to remain in sync with the needs of the users who find telehealth platforms useful. More comprehensive standards and regulations may be needed to ensure strong privacy and security protections for telehealth and all electronic consumer information [Hall 2014].

For users, ignorance in failing to read privacy policies and having concerns about digital privacy raises a few questions and chaos. It is important to note that the change in the framework and increasing consumer awareness would be a great addition to achieving the solution to this chaotic situation

References

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M. & Turner, E. (2020). Americans and privacy: Concerned, confused and feeling lack of control over their personal information. *Pew Research Center: Internet, Science & Tech.* URL: https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Bassan S. (2020). Data privacy considerations for telehealth consumers amid COVID-19. *Journal of Law and the Biosciences.* 7(1):lsaa075. doi:10.1093/jlb/lsaa075

Campos-Castillo, C. & Anthony, D.L. (2014). The double-edged sword of electronic health records: Implications for patient disclosure. *JAMA*. 22(e1). https://doi.org/10.1136/amiajnl-2014-002804

Campos-Castillo, C., Bartholomay, D.J., Callahan, E.F. & Anthony, D.L. (2016). Depressive symptoms and electronic messaging with health care providers. *Society and Mental Health*. 6(3):168-186. https://doi.org/10.1177/2156869316646165

Campos-Castillo, C. & Anthony, D. (2020). Racial and ethnic differences in self-reported telehealth use during the COVID-19 pandemic: A secondary analysis of a US survey of internet users from late March. *JAMA*. 28(1):119–125. https://doi.org/10.1093/jamia/ocaa221

Cauchi, D. (2011). Health insurance plan types and definitions. URL: https://www.ncsl.org/research/health/health-insurance-plan-types-and-definitions.aspx

Center for Democracy & Technology (2020, August 26). CDT & eHI Webinar – Draft Consumer Privacy Framework for Health Data. *YouTube*: https://www.youtube.com/watch?v=qL6KSKHR9QA

Cohen, I.G. & Mello, M.M. (2018). HIPAA and protecting health information in the 21st Century. *JAMA*. 320(3): 231. https://doi.org/10.1001/jama.2018.5630

Cohen, M.Z., Phillips, J.M. & Palos, G. (2001). Qualitative research with diverse populations. *Seminars in Oncology Nursing*. 17(3): 190-196. https://doi.org/10.1053/sonu.2001.25948

Earp, J.B., Anton, A.I., Smith, L.A. & Stufflebeam, W.H. (2005). Examining internet privacy policies within the context of user privacy values. *IEEE Transactions on Engineering Management*. 52(2): 227-237. doi:10.1109/TEM.2005.844927

Fetaji, M., Loskoska, S., Fetaji, B. & Ebibi, M. (2007). Investigating human computer interaction issues in designing efficient virtual learning environments. URL: https://telearn.archives-ouvertes.fr/hal-00190068/document

Fischer, S.H., Ray, K.N., Mehrotra, A., Bloom, E.L. & Pines, L.U. (2020). Prevalence and characteristics of telehealth utilization in the United States. *JAMA Network Open*. 3(10):e2022302. doi:10.1001/jamanetworkopen.2020.22302

Furstenberg, J. (2020). An investigation of the factors that contibute to the perceived likelihood of compliance with the HIPAA security rule among healthcare covered entities and business associates. *Nova Southeastern University NSUWorks*. URL: https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=2105&context=gscis_etd

Glenn, T. & Monteith, S. (2014). Privacy in the Digital World: Medical and health data outside of HIPAA protections. *Current Psychiatry Reports*. 16(11). https://doi.org/10.1007/s11920-014-0494-4

Goldstein, M. M. & Pewen, W. F. (2013). The HIPAA omnibus rule: Implications for public health policy and practice. *Public Health Reports*. 128(6), 554–558. https://doi.org/10.1177/003335491312800615

Greenleaf, G. (2014). Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories. *Journal of Law, Information and Science.* 23(1), 4-49. http://dx.doi.org/10.2139/ssrn.2280877

Guo, W., Rodolitz, J. & Birrell, E. (2020). Poli-see: an interactive tool for visualizing privacy policies. *Proceedings of the 19th Workshop on Privacy in the Electronic Society*. https://doi.org/10.1145/3411497.3420221

Hall JL & McGraw D. (2014). For telehealth to succeed, privacy and security risks must be identified and addressed. *Health Affairs*. 33(2); 216-221. doi: 10.1377/hlthaff.2013.0997

Huckvale, K., Prieto, J. T., Tilney, M., Benghozi, P.J. & Car, J. (2015). Unaddressed privacy risks in Accredited Health and Wellness Apps: A cross-sectional systematic assessment. *BMC Medicine*. 13(1). https://doi.org/10.1186/s12916-015-0444-y

Huckvale, K., Torous, J. & Larsen, M. E. (2019). Assessment of the data sharing and privacy practices of smartphone apps for depression and smoking cessation. *JAMA Network Open*. 2(4). https://doi.org/10.1001/jamanetworkopen.2019.2542

Is faceetime HIPAA compliant? *HIPAA Journal*. (2022). URL: https://www.hipaajournal.com/facetime-hipaa-compliant/

Jain, T. & Mehrotra, A. (2020). Comparison of Direct-to-Consumer telemedicine visits with primary care visits. *JAMA Network Open*. 3(12):e2028392. doi:10.1001/jamanetworkopen.2020.28392

Keenan A.J., Cert, G., Dip, G., Tsourtos, G. & Tieman, J. (2021). The Value of Applying Ethical Prinicples in Telehealth Practices: Systemic Reviews. *Journal of Medical Internet Research*. 23(3): e25698.

Kichloo, A., Albosta, M., Dettloff, K., Wani, F., El-Amir, Z., Singh, J., et al. (2020). Telemedicine, the current COVID-19 pandemic and the future: A narrative review and perspectives moving forward in the USA. *Family Medicine and Community Health*. 8(3). https://doi.org/10.1136/fmch-2020-000530

Largest Healthcare data breaches of 2021. (2021, December 30). *HIPAA Journal*. URL: https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2021/

Majumder, M.A. & Guerrini, C.J. (2016). Federal privacy protections: ethical foundations, sources of confusion in clinical medicine, and controversies in biomedical research. *American Medical Association Journal of Ethics*. 18(3): 288-298.

McDonald, A.M. & Cranor, L.F. (2008). The Cost of Reading Privacy Policies. *Journal of Law and Policy for the Information Society*. Privacy Year in Review Issue. URL: https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf

McGraw, D. & Mandl, K.D. (2021). Privacy protections to encourage use of health-relevant digital data in a learning health system. *NPJ Digital Medicine*. 4(1). https://doi.org/10.1038/s41746-020-00362-8

Mehrotra, A., Pines, L.U. & Lee, M.S. (2018). The dawn of direct-to-consumer telehealth. Rheuban, K. & Krupinski, E.A.(eds.), Understanding Telehealth. McGraw Hill. URL: https://accessmedicine-mhmedical-com.proxy.lib.umich.edu/content.aspx?bookid=2217&sectionid=187795446

Moretti, M. & Naughton, M. (2014). Why privacy policies are so inscrutable. *The Atlantic*. URL: https://www.theatlantic.com/technology/archive/2014/09/why-privacy-policies-are-so-inscrutable/379615/

Nass, S.J., Levit, L.A. & Gostin, L.O. (2009). The Value and Importance of Health Information Privacy. Institute of Medicine (US) Committee on Health Research and the Privacy of Health Information: *The HIPAA Privacy Rule*. editors. Washington (DC): National Academies Press (US).

Office for Civil Rights. (2020) Notification of Enforcement Discretion for Telehealth. HHS.gov. URL: https://www-hhs-gov.proxy.lib.umich.edu/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html.

Office for Civil Rights. (2021, June 28). Notification of enforcement discretion for telehealth. *HHS.gov*. URL:

https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html

Perlman, A., Zilberg, A.V., Bak, P., Dreyfuss, M., Leventer-Roberts, M., Vurembrand, Y. et al. (2020). Characteristics and symptoms of APP users seeking COVID-19–related digital health information and remote services: Retrospective cohort study. *Journal of Medical Internet Research*. 22(10). https://doi.org/10.2196/23197

Predmore, Z.S., Roth, E., Breslau, J., Fischer, S.H., & Pines, L.U. (2021). Assessment of patient preferences for telehealth in post–COVID-19 pandemic health care. *JAMA Network Open*. 4(12). https://doi.org/10.1001/jamanetworkopen.2021.36405

Ramirez, E. (2015). Privacy and the IoT: Navigating policy issues. *CES Opening Remarks, FTC public statement.*

Radtke, T., Haile, S.R., Dressel, H. & Benden, C. (2021). Covid-19 pandemic restrictions continuously impact on physical activity in adults with cystic fibrosis. *PLoS ONE*. 16(9): e0257852. https://doi.org/10.1371/journal.pone.0257852

Seh, A.H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., et al. (2020). Healthcare data breaches: Insights and implications. *Healthcare*. 8(2), 133. https://doi.org/10.3390/healthcare8020133

Schaub, F., Balebako, R., Durity, A.L., Cranor, L.F. (2015). A Design Space for Effective Privacy Notices. *USENIX Association*. URL: https://www.usenix.org/system/files/conference/soups2015/soups15-paper-schaub.pdf

Schwartz, P.M. & Solove, D. (2009) Notice & Choice. In The Second NPLAN/BMSG Meeting on Digital Media and Marketing to Children. URL: https://www.changelabsolutions.org/sites/default/files/documents/Notice_and_choice.pdf

Shachar, C., Engel, J., & Elwyn, G. (2020). Implications for telehealth in a postpandemic future. JAMA, 323(23), 2375. https://doi.org/10.1001/jama.2020.7943

Siedlecki, S.L. (2020). Understanding descriptive research designs and methods. *Clinical Nurse Specialist*. 34(1), 8–12. https://doi.org/10.1097/nur.0000000000000493

Stephens J. (2019). California Consumer Privacy Act. URL: https://www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_9/

Theodos, K. & Sittig, S. (2021) Health information privacy laws in the digital age: HIPAA doesn't apply. *Perspectives in Health Information Management.* 18(Winter): 1l.

2017 Global Mobile Consumer Survey: US edition. (2017). URL: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-2017-global-mobile-consumer-survey-executive-summary.pdf?pStoreID=hpepp

Watzlaf, V.J.M., Zhou, L., DeAlmeida, D.R., & Hartman, L.M. (2017). A systematic review of research studies examining telehealth privacy and security practices used by healthcare providers. *International Journal of Telerehabilitation*. 9(2), 39–58. https://doi.org/10.5195/ijt.2017.6231

Guo, W., Rodolitz, J., & Birrell, E. (2020). Poli-see: An interactive tool for visualizing privacy policies. In 19th Workshop on Privacy in the Electronic Society (WPES ’20). Virtual Event, USA. *ACM* New York. 15 pages. https://doi.org/10.1145/3411497.3420221

Zhou, L., Thieret, R., Watzlaf, V., Dealmeida, D. & Parmanto, B. (2019). A telehealth privacy and security self-assessment questionnaire for telehealth providers: development and Validation. *International Journal of Telerehabilitation*. 11(1):3-14. doi: 10.5195/ijt.2019.6276

Appendix 1

	7 Cups	98Point 6	Amwell	BCBSM	BetterHelp	Brightside	LiveHealth Online	Lemonaid	Khealth	Demand on Doctors	MDLive	PlushCare	Talkspace	Teladoc
Healthcare Providers														
No guarantee about providers and/or information on site	Yes	Didn't mention	Yes	Yes	Yes	Yes	Didn't mention	Yes	Yes	Yes	Yes	No	Didn't mention	Didn't mention
Providers are vetted and licensed	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Yes	Didn't mention
Providers responsible on mangaing data	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Yes	Yes	Didn't mention	Didn't mention	Didn't mention
Technical														
Guarantee data transfer/storage safety	Didn't mention	Didn't mention	No	No	No	Didn't mention	Didn't mention	No	No	No	Didn't mention	No	Yes	Yes
Guarantee downloads from site are virus free	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	No	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention
Use cookies/web beacons	Yes	Yes	Yes	Didn't mention	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Didn't mention	Yes
Data														
Data transfer and sharing	Yes	Yes	Yes	Didn't mention	Yes	Yes	Didn't mention	Yes	Didn't mention	Yes	Didn't mention	Diddn't mention	Didn't mention	Yes
Obtain information from third party and combine with our info	Didn't mention	Yes	Didn't mention	Didn't mention	Didn't mention	Yes	Didn't mention	Didn't mention	Yes	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention
Share identify info to third party	Didn't mention	No	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Yes	Yes	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention
Share information with subsudiary or parent company	Didn't mention	Yes	Didn't mention	Didn't mention	Yes	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Yes	Yes	Didn't mention	Didn't mention	Didn't mention
Users' rights														
Can withdraw consent for use of stored data	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Yes
Delete data	Yes	Didn't mention	Didn't mention	Didn't mention	Yes	Didn't mention	Didn't mention	No	Yes	Yes	Yes	Yes	Yes	Yes
Disable cookies	Yes	Yes	Yes	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Yes	Didn't mention	Yes	Yes	Yes	Didn't mention	Yes
Notify user of security breach	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Yes	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Yes	Didn't mention
Right to object for use of personal data in marketing	Yes	Yes	Didn't mention	Didn't mention	Yes	Didn't mention	Didn't mention	Yes	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Doesn't apply
Provides user data on request back to user	Yes (only california)	Didn't mention	Yes (only california)	Didn't mention	Yes (only california)	Didn't mention	Didn't mention	May/May not	Yes (only california)	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention
Confusing														
Confusing corporate/service structure	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Yes	Yes	Didn't mention	Yes	Didn't mention
Need to sign doc for using service	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	No	Didn't mention	Yes
Photos and videos uploaded become site IP without royalty	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	No	No	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Yes	Didn't mention
Use service at user own risk	Yes	Didn't mention	Didn't mention	Didn't mention	Yes	Didn't mention	Didn't mention	Yes	Didn't mention	Didn't mention	Didn't mention	Yes	Didn't mention	Didn't mention

Appendix 1

Contradictory														
Change privacy policy at any time	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Yes	Didn't mention	Didn't mention	Yes	Didn't mention	Yes	Didn't mention	Didn't mention	Didn't mention	Yes
Hold harmless and indemnify us	Yes	Didn't mention	Didn't mention	Didn't mention	Yes	Didn't mention	Didn't mention	Yes	Didn't mention	Didn't mention	Didn't mention	Yes	Didn't mention	Didn't mention
No service to Medicare or Medicaid	Didn't mention	Didn't mention	Yes	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention
Provide personal info at your own risk	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Yes	Yes	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention
Take inperson care (even if platform say otherwise)	Didn't mention	Didn't mention	Didn't mention	Yes	Yes	Yes	Didn't mention	Yes	Yes	Yes	Didn't mention	Yes	Didn't mention	Didn't mention
TMH platforms rights														
Cannot test or compromise security of site	Didn't mention	Didn't mention	Yes	Didn't mention	Yes	Didn't mention	Didn't mention	Yes	Didn't mention	Didn't mention	Yes	Didn't mention	Yes	Didn't mention
Discontinue service at any time without reason	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Yes	Yes	Yes	Yes	Yes	Didn't mention	Didn't mention	Yes	Yes	Didn't mention
Dispute to settle in arbitration	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Yes	Didn't mention	Didn't mention	Yes	Didn't mention	Yes	Didn't mention
No endorsement of any product on site (medication, professional)	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Didn't mention	Yes	Yes	Didn't mention	Yes	Didn't mention	Yes	Didn't mention	Didn't mention	Didn't mention

Footnote:
Yes/No/Didn't mention: act in accordance with the sub-themes
May/may not: gives double meaning

Appendix 2

S. No.	Theme	Platform	Statement
1	Healthcare Provider (No guarantee about providers and/or information on site)	Doctor on Demand (terms of service, p2)	*"The Healthcare Professionals who deliver Services through Doctor On Demand are independent professionals practicing within a group of independently owned professional practices collectively known as "Doctor On Demand Professionals". Doctor On Demand, Inc. does not practice medicine or any other licensed profession, and does not interfere with the practice of medicine or any other licensed profession by Healthcare Professionals, each of whom is responsible for his or her services and compliance with the requirements applicable to his or her profession and license."*
2	Healthcare Provider (No guarantee about providers and/or information on site)	Amwell (terms of service, p1)	*"Amwell does not make any representations or warranties about the training or skill of any Providers using the Services. You are ultimately responsible for choosing your particular Provider on the Services."*
3	Healthcare Provider (Providers are vetted and licensed)	Talkspace (terms of service, p4)	*"Talkspace does not directly employ the Providers matched through the Service. Talkspace created a modern, digital health network of nationwide digitally trained and accredited Providers. The Talkspace Network only works with independent, licensed, insured and vetted professional Providers."*
4	Technical (Guarantee data transfer/storage safety)	K Health (terms of service, p14)	*"However, we cannot guarantee that unauthorized third parties will never be able to defeat our security measures or use your personal information for improper purposes. You acknowledge that you provide your personal information at your own risk."*
5	Technical (Guarantee downloads from sites is a virus-free)	Lemonaid (terms of service, p8)	*"Lemonaid Health cannot and does not guarantee or warrant that email or files available for downloading from its Site will be free of viruses or other code that may contaminate or destroy data on*

Appendix 2

			your computer. You are responsible for implementing sufficient protective procedures and checks to maintain the accuracy of your data for maintaining a data back-up or other means for the reconstruction of any lost data."
6	Data (Data Transfer and sharing)	98Point6 (privacy policy, p5)	*"If we believe your actions are inconsistent with our user agreements or policies, or to protect the rights, property and safety of 98point6 or others; in connection with, or during negotiations of, any merger, sale of company assets, or acquisition of all or a portion of our business by another company."*
7	Data ('Obtain information from the third party and combining with users' info)	Brightside (privacy policy, p5)	*"Through our Services, we may allow third party advertising partners to set Technologies and other tracking tools to collect information regarding your activities and your device (e.g., your IP address, mobile identifiers, page(s) visited, location, time of day). We may also combine and share such information and other information (such as demographic information and past purchase history) with third party advertising partners. These advertising partners may use this information (and similar information collected from other websites) for purposes of delivering targeted advertisements to you when you visit third party websites within their networks."*
8	Data (Share identifying info to third-parties)	K Health (privacy policy, p5)	*"We may use your Personal Information in order to improve our AI models, so that we are constantly improving the information we provide our users. When you are using K, you are not only learning from people like you, they are also learning from you and your experiences. Over the long term, this growing repository of health experiences and clinical decision-making will accelerate medical research and improve our understanding of human disease."*
9	Data (Sharing information with	MDLive (privacy policy, p1)	*"MDLIVE is not a medical group. Any telemedicine consults obtained hrough our Website or Application*

Appendix 2

	subsidiary or parent company)		*are provid medical practitioners including, but not limited to, MDLIVE Medical Group, P.A., MDLIVEMedical Group (DE), P.A., MDLIV New York, MDLIVE Medical Group (IL), LLC, MDLIVE Medical Group(NC), P.C., MDLIVE Medical Group (NJ), LLC, MDLIVE M LLC, MDLive Medical Group of California,and MDL Medical Group (TX), PLLC (collectively, "MDLIVE Medical Group"), whi medical groups with a network of United States based health care providers (each, a "Provider"). MDLIVE Medical Group medical provider if you do not use a MDLIVE Medical Group Provider) is responsible for providing you with aNotice of Pr describing its collection and use of your health information, not MDLIVE. If you do not agree to be bound by those terms authorized to access or use our Website, and you must promptly exit our Website or Application."*
10	Users' rights (Can withdraw consent for the use of stored data)	Teladoc (privacy policy, p3)	"Subject to applicable law, you may withdraw your consent to uses and disclosures of Personal Information as outlined in this Privacy Policy. You must submit your request in writing to Teladoc. Withdrawing consent does not invalidate consent to any collection, use or disclosure of Personal Information to which you consented before consent was withdrawn. If you withdraw consent, or refuse further consent, Teladoc's ability to offer services to you may be limited.
11	Users' rights (Delete data)	Lemonaid (privacy policy, p4)	"We are unable to delete information from your medical record. At your request, we can deactivate your secure account so that you and others can no longer access it with your username and password."
12	Users' rights (Disable cookies)	Doctor on Demand (privacy policy, p2)	*"You can opt-out of Mixpanel's automatic retention of data collected through your browsers while on our Site. To track opt-outs, Mixpanel uses a persistent opt-out Cookie placed on your devices. You can find*

Appendix 2

			out the types of information AppsFlyer collects and how you can opt-out of AppsFlyer."
13	Users' rights (Notify user of a security breach)	Talkspace (privacy policy, p7)	*"At Talkspace, we will provide our Clients notice of any data breach and we employ a full time security O~cer, as w. ell as engaging a third party security ~rm to periodically audit both or code and technology security as well as our HIPAA policies and procedures around data security."*
14	Users' rights 2 (Provides user data on request back to the user)	Amwell (privacy policy, p3)	*"California residents are entitled once a year, free of charge to request and obtain certain information regarding our disclosure, if any, of certain categories of personal information to third parties for their direct marketing purposes in the preceding calendar year. We do not share personal information with third parties for their own direct marketing purposes."*
15	Confusing (Confusing corporate/service structure)	MDLive Privacy policy, p 10)	*"MDLIVE Medical Group provides the clinical services for MDLIVE, Inc. MDLIVE Medical Group is an independent, physician-owned m national network of United States based providers who provide clinical telehealth services. The MDLIVE Medical Group provides clin MDLIVE, Inc. platform to customers of MDLIVE, Inc."*
16	Confusing (Need to sign doc for using service)	Teladoc (terms of service, p1)	*"By using this site and the Teladoc service, you signify your acceptance of the Teladoc, Inc. and Teladoc Privacy Policy. If you do not agree to this policy, you should not use our service. If Teladoc, Inc. decides to change the Privacy Policy, we will post those changes prominently so users are always aware of what information we collect, how we use it, and under what circumstances, if any, we disclose it. We do, however, recommend that you read this Privacy Policy each time you use our Web site in case you missed our notice of changes to the Privacy Policy. Your continued use of the services and site*

Appendix 2

			following the posting of changes to these terms will mean you accept those changes."
17	Confusing (Photos and videos uploaded become site IP without royalty)	LiveHealth Online (terms of service, p5)	*"DIGITAL MILLENNIUM COPYRIGHT ACT HMC respects the intellectual property of others and expects users of our website to do the same. If you believe that your copyrighted work has been copied in a way that constitutes copyright infringement and is accessible on this site or through this service, you must provide the following information when providing notice of the claimed infringement to HMC."*
18	Confusing (Use service at your own risk)	PlushCare (terms of service, p10)	*"You agree to indemnify and hold PlushCare, its subsidiaries, affiliates (including the Providers), officers, agents, and other partners and employees, harmless from any loss, liability, claim, or demand, including reasonable attorney's fees, made by any third party due to or arising out of (a) your use of the Websites or the Service in violation of this Agreement, (b) your failure to comply with applicable laws and regulations; and/or (c) your breach of this Agreement and/or any breach of your representations and warranties set forth above."*
19	Contradictory (Change privacy policy at any time)	BetterHelp (privacy policy, p15)	*"Regardless of changes to our Privacy Policy, we will never use the information you submit under our current privacy notice in a new way without first notifying you and giving you the option to stop using the Platform. Your continued use of our websites and services following the posting of changes constitutes your acceptance of such changes."*
20	**Contradictory** (Hold harmless and indemnify us)	BetterHelp (terms of service, p4)	*"You will indemnify us, defend us, and hold us harmless from and against any and all claims, losses, causes of action, demands, liabilities, costs or expenses (including, but not limited to, litigation and reasonable attorneys' fees and expenses) arising out of or relating to any of the following: (a) your access to or use of the Platform; (b) any actions made with*

Appendix 2

			your account or Account Access whether by you or by someone else; (c) your violation of any of the provisions of this Agreement; (d) non-payment for any of the services (including Counselor Services) which were provided through the Platform; (e) your violation of any third party right, including, without limitation, any intellectual property right, publicity, confidentiality, property or privacy right. This clause shall survive expiration or termination of this Agreement."
21	Contradictory (No service to Medicare or Medicaid)	Amwell (terms of service, p1)	*"You hereby certify that you are not a Medicare or Medicaid beneficiary. If you provide false or deceptive information regarding your Medicare or Medicaid enrollment status, Amwell reserves the right to terminate all current or future use of the Services by you."*
22	Contradictory (Provide personal info at your own risk)	Lemonaid (privacy policy, p2)	*"You acknowledge that you provide your personal information at your own risk. Remember, emails and SMS/text messages we send you aren't secure because they aren't encrypted."*
23	Contradictory (Take in-person care (even if the platform says otherwise)	Brightside (terms of service, p5)	*"None of the Site content (other than personalized information you receive directly from Healthcare Providers) should be considered medical advice or an endorsement, representation, or warranty that any particular medication or treatment is safe, appropriate, or effective for you. BRIGHTSIDE DOES NOT RECOMMEND OR ENDORSE ANY SPECIFIC DRUGS, TESTS, HEALTHCARE PROVIDERS, PRODUCTS, PROCEDURES, OPINIONS, "OFF-LABEL" DRUG USES, OR OTHER INFORMATION THAT MAY BE MENTIONED through Services and does not represent that any Services provided on the Site are an appropriate substitute for direct in-person services in all cases."*

Appendix 2

24	Platform rights (Cannot test or compromise the security of the site)	Amwell (terms of service, p2)	*"You may not access or use, or attempt to access or use, the Services to take any action that could harm us or any third party, interfere with the operation of the Services, or use the Services in a manner that violates any laws."*
25	Platform rights (Discontinue service at any time without reason)	Talkspace (terms of service, p7)	*"Talkspace may suspend or terminate your access to the Service at any time, for any reason or for no reason at all. Talkspace has the right (but not the obligation) to refuse to provide access to the Service to any person, agency, or organization at any time, for any reason or for no reason at all, in our sole discretion. Talkspace reserves the right to change, suspend, or discontinue all or part of the Service, temporarily or permanently, without prior notice."*
26	Plaatform rights (Disputes to settle in arbitration)	Talkspace (terms of service, p9)	*"Any dispute or claim relating in any way to your use of the Talkspace Service will be resolved by binding confidential arbitration, rather than in court. The Federal Arbitration Act and federal arbitration law apply to these Terms. There is no judge or jury in arbitration, and court review of an arbitration award is limited. However, an arbitrator can award on an individual basis the same damages and relief as a court (including injunctive and declaratory relief or statutory damages) and must interpret these Terms as a court would."*
27	Platform rights (No endorsement of any product on site (mediation or professional)	LiveHealth Online (terms of service, p1)	*"Neither HMC, nor any of its licensors or suppliers, shall be liable for any advice obtained from a health service provider using LiveHealth Online. HMC does not recommend or endorse any specific providers, tests, medications, products, or procedures. All services or recommendations made by a health service provider are based on their independent professional judgment."*