2023 16th International Conference on Security of Information and Networks (SIN) | 979-8-3503-4321-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/SIN60469.2023.10475119

Data Leaks to Third-Party Services on Medical Websites

Sampsa Rauti
Department of Computing
University of Turku
Turku, Finland
sjprau@utu.fi

Esko Vuorinen
Department of Computing
University of Turku
Turku, Finland
etvuor@utu.fi

Robin Carlsson
Department of Computing
University of Turku
Turku, Finland
crcarl@utu.fi

Panu Puhtila
Department of Computing
University of Turku
Turku, Finland
papuht@utu.fi

***Abstract*—Several web-based healthcare services such as medical center websites, online pharmacies and mental health websites process sensitive medical data that should not end up in the wrong hands. Today's trend of incorporating several third-party services on websites poses a threat to online privacy, and this is also a considerable risk when it comes to medical websites. In this study, we conduct a network traffic analysis on 20 Finnish healthcare websites to investigate the types of personal data that these websites inadvertently share with third parties and to identify these third-party entities. Our results indicate that even without consent, 12 of these websites leak sensitive data to third parties. We also discuss the implications of health data leaks and offer recommendations for web developers to prevent such privacy issues in the future.**

***Index Terms*—Medical websites, data leaks, data concerning health, web privacy, third-party services**

I. Introduction

In today's world, digital technologies have become an integral part of our daily lives, significantly impacting our activities in numerous ways. People increasingly rely on digital technologies as a tool that delivers various essential services for customers who cannot or do not want to use services onsite. Digital services can have advantages for many vulnerable groups such as the elderly, people with severe medical conditions, and individuals living in remote areas can benefit from digital services [1], [2]. Legislators have also passed laws aiming to improve the availability and quality of the essential digital services. For instance, the Act on the Provision of Digital Services (306/2019) was established in Finland in 2019 to allow citizens to use them in an equal and secure manner. The recent COVID-19 pandemic has accelerated the digital shift even more and the demand for using essential services online has only become more apparent [3].

However, these essential web services process highly sensitive medical data that should not end up in the wrong hands. At the same time, modern websites are built by making use of several third-party services (such as web analytics and performance measurement tools). Without web developers and organizations maintaining the websites realizing, users' delicate health related data can be sent to these third parties. These kinds of data leaks have great potential to cause harm for individuals.

The General Data Protection Regulation (GDPR), a data protection law implemented by the European Union (EU), recognizes the sensitivity of an individual's medical information as a special category of personal data, known as ”data concerning health.” [4] The definition encompasses information such as a person's physical and mental health, medical conditions, treatments, medications, test results, and other details related to health. This data should be subject to heightened protection. Organizations that process this data must implement the ”appropriate technical and organizational measures” to safeguard users' privacy and personal data. According to GDPR, except for a few exceptions, an explicit consent has to be obtained from an individual before processing of health data [5]. In the light of the sensitive nature of health data and the GDPR, it is interesting to see how well the health data is being protected on medical websites.

In this paper, we assess the privacy of medical websites and study if health related data is being leaked to third parties. More specifically, we experiment with 20 Finnish websites of medical centers, online pharmacies and mental health related websites and perform a network traffic analysis to reveal potential third-party data leaks happening without the user's consent. We study the nature of personal data sent to third parties and who these third parties are. Furthermore, we also take a look at the privacy policies of the studied websites to see whether they correspond to the recorded network traffic and transparently inform the users how their data is being processed. Our findings contribute to the field of privacy research by providing valuable insights on practical health data leaks to third parties and also have important societal impact, as many of the studied organizations are already in the progress of improving the privacy of their websites.

The rest of the paper is organized as follows. Section II reviews the related work. Section III outlines the study setting and methods. Section IV presents the results of network traffic analysis, detailing the nature of found data leaks and the involved third parties. Section V discusses the implications of health data leaks and provides recommendations for improving the software development process from a privacy point of view. Section VI concludes the paper.

This research has been funded by Academy of Finland project 327397, IDA – Intimacy in Data-Driven Culture.

II. Related Work

Prior research on data tracking by third parties and related data leaks in medical websites, applications and IoT systems is plentiful, and concerns brought forth by this research have had a role in shaping the current legislative situation concerning the user privacy and data collection. While not exhaustive, the list of previous studies presented here gives a good idea on how the particular phenomenon of third-party services on medical websites has been approached before.

Already in 2012, when the use of web analytics tools was not yet that widespread, Masters [6] addressed the issue of third-party analytics tools being present in medical websites, and how these tools collected user information without adequately notifying or obtaining consent from the users. In the following year, Huesch published a paper detailing similar findings related to searching for medical information [7]. Concurrently, Brown and Levy [8] published their research which presented a design for an instrument to benchmark the actual and documented information collection practices of pharmaceutical websites. During the same period, Burkell and Fortier [9], [10] proved how medical websites did not correctly disclose their data tracking practices, leading to falsely given consent to such activities, and how consumer health websites habitually tracked their users with analytics tools to build detailed profiles of them.

The recent years have seen the publication of several papers related to our research. Surani et al. [11] examined mental health web services, and concluded that the majority of them had severe deficiencies in their privacy policies. Zheutlin et al. [12] inspected how USA-based government, non-profit and commercial health-related websites tracked the user data with third-party cookies. Friedman et al. [13] recently published a paper on how third-party tracking technologies in hospital websites jeopardize the user privacy and pose a legal liability for the hospitals in question. A similar theme was addressed by Yu et al. [14], who conducted a large-scale automated survey on hospital websites across the globe, revealing that 53.5% of them deployed tracking tools that collected data on their users. Friedman et al. studied in their 2022 research letter [15] the prevalence of third-party tracking tools in abortion clinic websites, and found that the majority of them (99.1%) included some form of tracking tool that leaked user data to third parties. Huo et al. [16]. demonstrated in their paper studying the privacy of patient web portals that 14% of them leaked data as sensitive as names and phone numbers to third parties.

Schnell and Roy investigated in their 2022 paper [17] whether the design on hospital websites made it harder to actually find the privacy policy, and thus to be properly informed about the data collection to consent to it. Wesselkamp et al. [18] designed a browser extension in 2021 to detect third-party tracking cookies used on websites and then conducted a research with it to inspect 385 medical websites operating in the EU area. They discovered that 62% of the studied websites deployed tracking tools before the consent to data collection was given by the user, and 15% even after the consent had been rejected.

On the other hand, there is also research that aims to prove that actually the collection of user data in medical websites is beneficial for the user, such as Kes et al. [19]. In their paper, they argue that it is good that health-related websites collect their users data, even when violating the privacy of the user, as this leads to the website becoming ”more accustomed” to the user. Kes et al. see this as akin to a relationship that might build between a regular customer and the real-life pharmacist, a relationship which might be useful for the customer since they benefit by getting better and more precise service and help. It is debatable whether such ”benefits” ever really materialize in this kind of online customer relationship, and considering the very real risks associated with the user data being leaked to third parties it is quite questionable whether such arguments can even be made in good faith. In the current legislative trend and especially within the framework of the EU's GDPR, however, such data leaks without the user's consent are problematic, and leaking sensitive data concerning health to actors such as Google and Facebook/Meta cannot be justified.

In comparison to the previous research, our paper takes a detailed approach to studying data leaks on medical websites, providing an elaborate analysis of personal data leaking to third parties. Unlike many of the previous studies, we also study what personal data is transmitted to third parties despite rejecting cookies and data collection. Moreover, we provide an overview of privacy in different categories of web-based health services in Finland.

III. Study Setting

In the current study, the privacy of 20 Finnish medical websites is assessed. The studied websites include the websites of 8 medical centers, 7 mental health services, and 5 online pharmacies. Instead of covering a large number of websites, our objective here is to provide a detailed analysis of health data leaks, their contents and third parties receiving data.

To evaluate the privacy of the medical websites and study potential data leaks, we ran a brief testing sequence on the studied websites, testing the most critical functionalities of the selected services. The testing sequence was performed manually with the Google Chrome browser. First, all cookies and data collection were rejected on the websites. In other words, we only accepted minimal possible cookies and data collection. Although it is likely many users consent to data collection without much forethought, the setting we chose aims to demonstrate that even with strict privacy settings, websites handling highly sensitive data can still leak information to third parties.

The testing sequence we performed depended on the type of website in question[1]:

- *Medical centers.* Starting from the main page, a search (e.g. a specific medical condition such as depression) was

[1] We have also recorded the exact test sequences for each website and they are available upon request.

first performed and an information page was navigated to from the search results page. Lastly, we also visited and tested the appointment booking page, filling in information such as the required service (for example, seeing a doctor with specific specialization or getting vaccinated), date of appointment, location of medical center etc. The appointment booking process was aborted before an actual appointment was made, but our test sequence still showed an intention to make an appointment to potential third parties.

- *Mental health websites.* A search was carried out on the front page, after which a search result was chosen and clicked on in order to reach an information page on a specific topic (e.g. depression). After this, a page indicating the user is looking into options for seeking help was navigated to – for example, in some instances this was an appointment booking page, in some cases simply a page containing a phone number for mental health helpline. Like with medical center websites, if there was a page for booking an appointment, we filled in some information to see whether it was leaked and continued as far as possible without making an actual appointment.
- *Online pharmacies.* On the main page, we searched for a specific prescription medicine with the search function. We then navigated to a product page describing the medicine, and finally proceeded to order the medicine – but aborted the process before an actual order was made. This test sequence, therefore, was designed to simulate the user's intent to order a specific prescription medicine from the studied pharmacy.

To record the network traffic generated by the websites, we made use of Google Chrome's Developer Tools. While recording the traffic, we disabled the cache to avoid any distortions in test results caused by the presence of data cached previously. From the traffic recording, we extracted only the requests delivered to third-party services. The recorded traffic was stored in log files for further analysis. The log files were then manually examined and all instances of personal data were documented. We were looking for two kinds of personal data:

- Data that can be used to uniquely identify the user of the website, such as IP addresses and device specific identifiers. Identifying data can also be a combination of several technical details such as operating system, browser, window size, etc.
- Sensitive contextual data, for instance an URL address showing that the user has displayed or intended to order a specific prescription medicine from an online pharmacy. Another example of sensitive contextual data on medical webpages is data associated with booking a doctor's appointment.

The worst data leaks happen when these two types of personal data, identifying and sensitive contextual data are collected together and combined by a third party. This makes it possible for the third party to deduce that the user seeks a specific type of help, is likely to have a specific medical condition, or orders a particular medicine. We focus on these kinds of data leaks in this study.

In addition to analyzing network traffic, the privacy policy documents and cookie banners of the websites were also examined. The privacy policies and cookie banners were studied to gauge whether data sharing with third parties was sufficiently covered. The transparency of privacy policy documents was assessed by studying whether their contents aligned with our findings in the actual network traffic. In particular, in the cases in which data concerning health was shared with third parties, the privacy policies and cookie banners were studied in order to see whether this aspect of the data processing was adequately reported to users.

Finally, because ”personal data” is a pivotal concept in the context of data leaks, this term requires brief clarification. Here we use the same definition as the GDPR and the Finnish Office of the Data Protection Ombudsman. According to these sources, *personal data* is ”all data related to an identified or identifiable person”[2]. By this definition, data items such as device specific identifiers, IP addresses, accurate location data or any piece of data identifying the website visitor counts as personal data. Moreover, although many technical data items such as operating system, browser version or screen resolution alone are not enough to uniquely identify someone, by combining these details, third parties can use them for identification. For that reason, the definition of personal data also encompasses these details.

IV. Results

Figure 1 shows the third-party services receiving sensitive data on the studied medical websites. We can see that Google is the most frequently appearing third party, receiving confidential personal data on 8 websites. Facebook/Meta, React&Share (a customer feedback tool), and Algolia (a search-as-a-service platform) come second with 2 occurrences. In addition, there are 9 miscellaneous services appearing only once.

The *mental health websites*, shown in Figure 2, also leaked a lot of sensitive personal data even with no consent. In total, 5 out of 7 mental health websites had data leaks. Addresses of visited pages, such as information pages on mental health conditions, leaked regularly (in 5 out of 7 cases), often to two separate third parties. Search terms, which may contain information about the user's mental health conditions, leaked in 4 out of 7 cases. Finally, 3 websites out of 7 leaked the user's visit to a help-seeking page.

The studied mental health websites included public sector services as well as websites from private and third sector (nonprofit sector, e.g. mental health associations). Although our sample size is small, it is easy to make an observation that public sector web services (MH1 and MH2) are doing much

[2] See the definitions at https://gdpr.eu/eu-gdpr-personal-data/ and https://tietosuoja.fi/en/what-is-personal-data

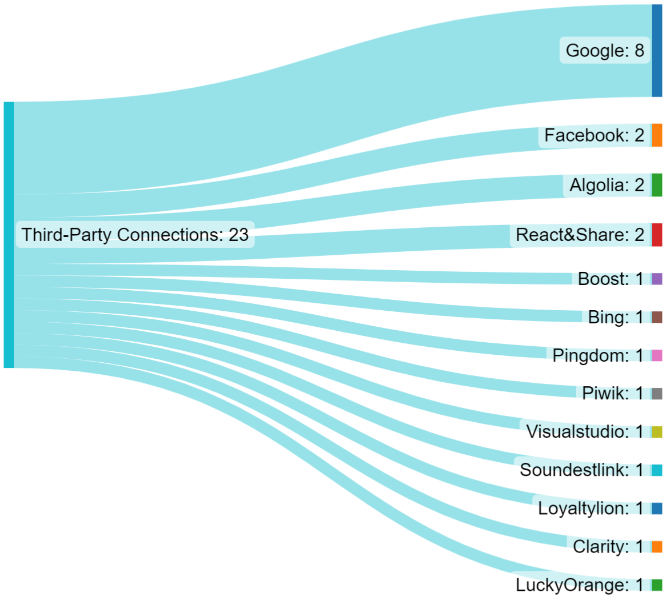

Fig. 1. Third parties receiving sensitive personal data on medical websites.

better than services of other sectors. No third-party services collecting sensitive data were detected on these websites. The third sector (MH3, MH4, and MH5) seems to fare slightly worse than the private sector (MH6 and MH7). It is likely that the associations often do not have the necessary resources and expertise to understand and fix privacy issues, although it would be very important to implement the necessary steps to resolve these privacy concerns.

The *medical center websites* and their data leaks are shown in Figure 3. Although consent was not given, 6 out of 8 medical center websites leaked sensitive personal data. URL addresses of pages visited by the user leaked in 5 out of 8 cases, potentially revealing the user's interest in specific medical conditions, particular treatments, or a specific doctor. The intent to seek help (usually a visit on an appointment booking page) was leaked on 4 out of 8 websites. Search terms potentially containing names of diseases or symptoms were leaked in 3 out of 8 cases. Finally, 3 websites out of 7 leaked the user's visit to an appointment booking page.

The majority of the studied *online pharmacies* did quite well in our experiments. Four of the five studied pharmacies did not use any third-party services on their websites with minimum consent. However, one of the studied pharmacies (OP1) leaked the visited page to 5 third parties and the search term (which is often likely to be a sensitive medicine name or symptom) to 6 separate third parties without consent! This was the worst individual outcome among all the studied websites. Upon further investigation, we also learned that OP1 leaked the name of the ordered medicine, customer's full name and email address to a third party (LoyaltyLion) during the medicine order process!

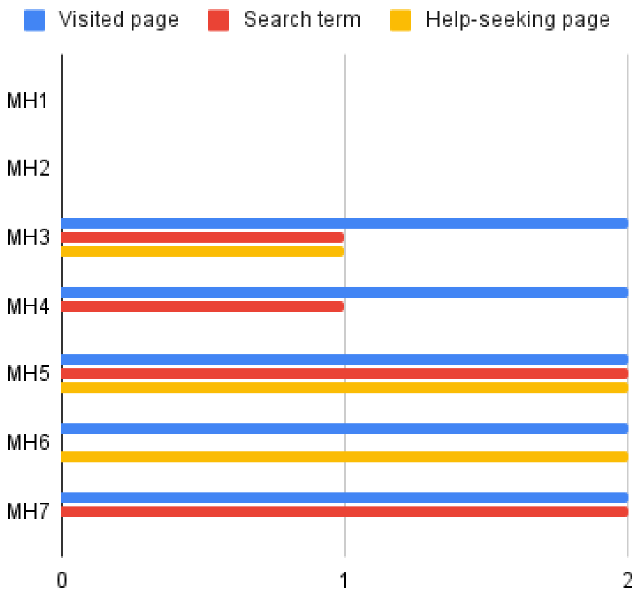

Fig. 2. Sensitive data leaks on mental health websites.

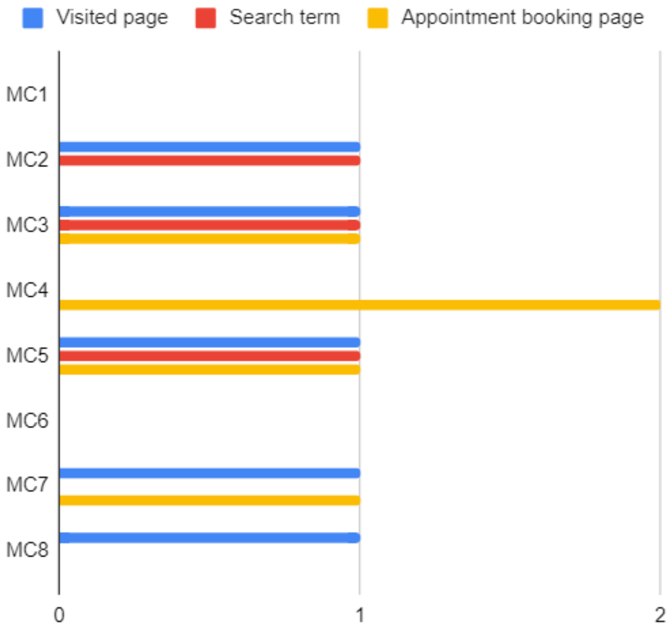

Fig. 3. Sensitive data leaks on medical center websites.

In total, 12 out of the 20 studied medical websites leaked sensitive data to third parties. The visited page was leaked in 11 cases. Visit on help-seeking (or appointment booking) page leaked in 7 cases and the search term in 8 cases. We consider these numbers alarmingly high, as the leaks contained sensitive personal data that was transferred without consent.

TABLE I
DISCREPANCIES BETWEEN THE ANALYZED PRIVACY POLICIES AND ACTUAL DATA COLLECTION.

Website	Unique identification mentioned	Current page mentioned	Third parties mentioned
MH3			
MH4			
MH5			
MH6	X	X	
MH7	X		X
MC2			
MC3	X	X	
MC4		X	
MC5	X	X	X
MC7	X		
MC8	X	X	X
OP1	X		

Table I shows the results of privacy policy analysis. The websites that were found to leak sensitive data are listed in the table. For each website, the table indicates whether users were informed about being uniquely identified, whether it was mentioned that the current page is sent to the third party, and whether all the third parties were named. Together, these details would at least inform users that their sensitive data may be leaked to third parties. As the sparsely filled table shows, privacy policies do not do a good job informing users about the data processing taking place on the websites. Only the privacy policies of MC5 and MC8 got a passing grade, even though they were somewhat vague about the first two details.

V. DISCUSSION

Medical services provided online have several advantages. They offer increased accessibility and expanded reach for many target groups, as web-based services allow healthcare providers to break down geographical barriers and extend their outreach to a broader population, particularly many vulnerable groups. These services are also cost-effective and flexible, since in many cases healthcare providers can optimize their schedule by organizing virtual appointments [20]. Online healthcare services are also frequently associated with anonymity, privacy and confidentiality. Unfortunately, the results of this study indicate that this trust may be largely misplaced when it comes to many online services.

A. Key findings

The key findings of the study can be summarized as follows:

- Even without consent, the studied medical websites send sensitive data (e.g. details on appointment bookings and searches with medicine names or medical conditions) to third-parties.
- In total, 12 out of 20 studied medical websites leaked personal data to third parties without consent.
- Google Analytics was the most frequent third party, collecting sensitive data in 8 cases out of 20.
- The fact that confidential search terms and visits on pages related to seeking help or booking appointments are recorded by third parties is especially concerning.

B. Implications of health data leaks

Individuals deem health data highly sensitive and personal, which makes leaking this data a serious privacy violation not only in law but also in an individual's mind. Very few people want information on their medical conditions, treatments, and medication to reach unauthorized sources. Health data leaks to unauthorized third parties strongly violate an individual's right to privacy rights, which can lead to a sense of vulnerability and loss of trust in medical websites and healthcare systems in general [21]. This can be especially detrimental to groups that are vulnerable to begin with.

If health data is delivered to several third parties, as was the case with many studied services, there is a greater chance it ends up in the wrong hands. Health data leaking and possibly becoming public knowledge can have various adverse effects, such impacting victims' personal and professional lives, and causing social exclusion. The individual could even be denied employment or insurance coverage, or otherwise experience biased treatment due to their health.

It is also not impossible that some third parties exploit health data leaks for financial gain. In theory, the data could be sold to another external party. Also, even if it is not shared with any further parties, leaked health data can be utilized for profiling users based on their health status. Such profiles can be used for targeted advertising, for instance. Health data is very valuable: if a user's credit card number leaks, the card can be replaced but health data can contain lots of information that stays valid forever.

C. Recommendations for web developers

The use of third-party analytics and collecting personal data from users, especially without consent, is difficult to justify on medical websites. While it is quite apparent the studied websites are not leaking sensitive data intentionally, there are several precautions web developers should take in order to prevent these kinds of serious data leaks from happening.

The best and obvious alternative would be to remove third-party analytics altogether, since a strong argument can be made that their place is not on websites handling sensitive personal data. If web analytics are needed, self-hosted services like Matomo can be used [22], [23]. By using such local analytics solutions, the company or organization retains full control over the collected data and it is not handed over to a third party.

All use of third-party services should be thoroughly evaluated in terms of their privacy and using them should be carefully justified. There are some well-justified cases for using third-party services such as trusted chat services or appointment booking systems. However, third-party analytics are not essential for the functionality of these websites in the same way.

As off-the-shelf platforms often used when developing modern websites often either have easy options to add third-party analytics services or include these services by default, developers may not always even be aware of their presence and implications. This is why the testing phase of the software development process should include a detailed examination of data leaking to third parties, much like what has been done in the current study. Especially the pages which process sensitive information such as the pages for booking appointments or ordering prescription medicines have to be carefully analyzed. The network traffic analysis gives the developers a realistic picture of what kind of data the third parties collect. This also helps the website maintainers to decide what third parties should be removed and provides a basis for transparent reporting of third parties and shared data in a privacy policy document.

Familiarity with the specific application area, in this case the healthcare sector, is also important. The development team needs to have an understanding of the privacy regulations on this specific field and also effectively communicate with the stakeholders to understand the requirements ensuring the safety of sensitive data. With critical services such as medical center websites and online pharmacies, it is also highly advisable to conduct an external privacy audit.

Finally, to avoid non-transparent privacy policies, companies and organizations should at the very least sufficiently inform the user that they are being identified by third-party services and contextual data about them is reported to external parties (e.g. the websites they view and actions they perform are recorded). The involved third parties should also be explicitly named. Using ready-made templates or checklists as a starting point when creating privacy policy documents would probably be helpful [24]. Another potential approach could be to use the co-design principle [25], in this instance to task a group of end-users who possess neither technical nor legal expertise to read the privacy policy to determine if it is understandable to the average consumer. It is worth noting, however, that even when the website visitors are adequately informed about data processing activities, transferring sensitive personal data to third parties can be argued to be unnecessary and unethical [26].

VI. Conclusion

In the current study, we have discussed data leaks on Finnish medical websites. Our results show that out of 20 studied websites, 12 websites leak sensitive identifying and contextual data that is often related to the visitor's health, even when the user accepts only minimal cookies and data collection. Even though our dataset in this study is moderately small, the result that 60% of the studied websites leak sensitive personal data shows that there are substantial privacy challenges in the web services in the Finnish healthcare sector. Unfortunately, these issues almost certainly extend far outside the websites we studied. Our future work involves analyzing the privacy of other medical web resources such as websites of Finnish healthcare districts.

We are hopeful that these concerning findings urge software developers and data protection officers involved in maintaining web-based healthcare services to pay more attention to third parties and privacy-by-design. It is crucial that web service developers and maintainers understand their responsibility for protecting customer's sensitive data. Clearly informing users of what personal data is processed and who the parties processing it are is also imperative. In web-based medical services, the use of any external service that potentially collects data, not to mention several of them, is not reasonable. If serious data leaks like the ones we found in this study are not addressed, this will only make vulnerable groups even more vulnerable online in terms of privacy. Any user of web-based medical services should be able to find these services as trustworthy as the traditional onsite healthcare system.

References

[1] T. Heponiemi, V. Jormanainen, L. Leemann, K. Manderbacka, A.-M. Aalto, and H. Hyppönen, "Digital divide in perceived benefits of online health care and social welfare services: national cross-sectional survey study," *Journal of medical Internet research*, vol. 22, no. 7, p. e17616, 2020.

[2] S. Somenahalli and M. Shipton, "Examining the distribution of the elderly and accessibility to essential services," *Procedia-social and behavioral sciences*, vol. 104, pp. 942–951, 2013.

[3] F. Almeida, J. D. Santos, and J. A. Monteiro, "The challenges and opportunities in the digitalization of companies in a post-covid-19 world," *IEEE Engineering Management Review*, vol. 48, no. 3, pp. 97–103, 2020.

[4] T. Mulder, "The protection of data concerning health in europe," *Eur. Data Prot. L. Rev.*, vol. 5, p. 209, 2019.

[5] S. McLennan, L. A. Celi, A. Buyx *et al.*, "Covid-19: putting the general data protection regulation to the test," *JMIR Public Health and Surveillance*, vol. 6, no. 2, p. e19279, 2020.

[6] K. Masters, "The gathering of user data by national medical association websites," *The Internet Journal of Medical Informatics*, vol. 6, no. 2, 2012.

[7] M. D. Huesch, "Privacy threats when seeking online health information," *JAMA Internal Medicine*, vol. 173, no. 19, pp. 1838–1840, 2013.

[8] S. D. Brown and Y. Levy, "Towards a development of an index to measure pharmaceutical companies' online privacy practices," *Online Journal of Applied Knowledge Management (OJAKM)*, vol. 1, no. 1, pp. 93–108, 2013.

[9] J. Burkell and A. Fortier, "Privacy policy disclosures of behavioural tracking on consumer health websites," in *Proceedings of the American Society for Information Science and Technology*, vol. 50, no. 1. Wiley Online Library, 2013, pp. 1–9.

[10] ——, "Consumer health websites and behavioural tracking," in *Proceedings of the Annual Conference of CAIS/Actes du congrès annuel de l'ACSI*, 2012.

[11] A. Surani, A. Bawaked, M. Wheeler, B. Kelsey, N. Roberts, D. Vincent, and S. Das, "Security and privacy of digital mental health: An analysis of web services and mobile apps," in *Conference on Data and Applications Security and Privacy*, 2023.

[12] A. R. Zheutlin, J. D. Niforatos, and J. B. Sussman, "Data-tracking on government, non-profit, and commercial health-related websites," *Journal of general internal medicine*, pp. 1–3, 2021.

[13] A. B. Friedman, R. M. Merchant, A. Maley, K. Farhat, K. Smith, J. Felkins, R. E. Gonzales, L. Bauer, and M. S. McCoy, "Widespread third-party tracking on hospital websites poses privacy risks for patients and legal liability for hospitals: Study examines the widespread use of third-party tracking on hospital websites and the privacy risks for patients and legal liability for hospitals," *Health Affairs*, vol. 42, no. 4, pp. 508–515, 2023.

[14] X. Yu, N. Samarasinghe, M. Mannan, and A. Youssef, "Got sick and tracked: Privacy analysis of hospital websites," in *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2022, pp. 278–286.

[15] A. B. Friedman, L. Bauer, R. Gonzales, and M. S. McCoy, "Prevalence of third-party tracking on abortion clinic web pages," *JAMA Internal Medicine*, vol. 182, no. 11, pp. 1221–1222, 2022.

[16] M. Huo, M. Bland, and K. Levchenko, "All eyes on me: Inside third party trackers' exfiltration of phi from healthcare providers' online systems," in *Proceedings of the 21st Workshop on Privacy in the Electronic Society*, ser. WPES'22. New York, NY, USA: Association for Computing Machinery, 2022, p. 197–211.

[17] K. Schnell and R. Kaushik, "Hunting for the privacy policy – hospital website design," 2022.

[18] V. Wesselkamp, I. Fouad, C. Santos, Y. Boussad, N. Bielova, and A. Legout, "In-depth technical and legal analysis of tracking on health related websites with ernie extension," in *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society*, ser. WPES '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 151–166.

[19] I. Kes, D. Heinrich, and D. M. Woisetschlager, "Behavioral targeting in health care marketing: Uncovering the sunny side of tracking consumers online," in *Let's Get Engaged! Crossing the Threshold of Marketing's Engagement Era: Proceedings of the 2014 Academy of Marketing Science (AMS) Annual Conference*. Springer, 2016, pp. 297–297.

[20] A. Ala, V. Simic, M. Deveci, and D. Pamucar, "Simulation-based analysis of appointment scheduling system in healthcare services: A critical review," *Archives of Computational Methods in Engineering*, vol. 30, no. 3, pp. 1961–1978, 2023.

[21] V. Rafe and M. Monfaredzadeh, "A qualitative framework to assess hospital/medical websites," *Journal of medical systems*, vol. 36, pp. 2927–2939, 2012.

[22] A. Chandler and M. Wallace, "Using Piwik instead of Google analytics at the Cornell university library," *The Serials Librarian*, vol. 71, no. 3-4, pp. 173–179, 2016.

[23] J. Gamalielsson, B. Lundell, S. Butler, C. Brax, T. Persson, A. Mattsson, T. Gustavsson, J. Feist, and E. Lönroth, "Towards open government through open source software for web analytics: The case of matomo," *JeDEM-eJournal of eDemocracy and Open Government*, vol. 13, no. 2, pp. 133–153, 2021.

[24] M. Rowan and J. Dehlinger, "A privacy policy comparison of health and fitness related mobile applications," *Procedia Computer Science*, vol. 37, pp. 348–355, 2014.

[25] E. B.-N. Sanders and P. J. Stappers, "Co-creation and the new landscapes of design," *CoDesign*, vol. 4, no. 1, pp. 5–18, 2008.

[26] P. M. Schwartz, "Privacy, ethics, and analytics," *IEEE security & privacy*, vol. 9, no. 3, pp. 66–69, 2011.