Original Article

Assessing Information Confidentiality in Telemedicine Platforms Using Public Web Data: A Case Study of Persian Televisit Websites

Mohammad Haddad Soleymani[1], MSc;
Adel Mohammadpour[2], PhD

[1]Department of Epidemiology and Biostatistics, School of Public Health, Tehran University of Medical Sciences, Tehran, Iran;
[2]Department of Mathematics and Statistics, University of Calgary, Calgary, Alberta, Canada

Correspondence:
Mohammad Haddad Soleymani, MSc;
Poursina Ave., Qods Ave., Enghelab Ave.,
Postal code: 1417613151, Tehran, Iran
Tel: +98 21 88989123
Email: m-haddadsoleymani@alumnus.tums.ac.ir
Received: 28 December 2024
Revised: 03 May 2025
Accepted: 04 July 2025

Abstract

Background: The shift from traditional office visits to internet-based care has accelerated during the COVID-19 pandemic, increasing reliance on telemedicine platforms. This growth has led to more health-related electronic data and heightened risks of unauthorized access, making it essential to prioritize information confidentiality issues. This study aims to reveal the disclosure of confidential information on a Persian televisit website.

Methods: In this observational case study, we gathered public health-related electronic data from a Persian televisit website in 2022. SAS software was used to harvest messy data about patients and doctors and create a structured dataset. Meanwhile, Microsoft Excel and RStudio software programs were used for data visualization. A hashing algorithm was applied to encode personal information, preventing the identification of individuals.

Results: Our study showed how public web data about 263 patients and 194 doctors, harvested from the target website, can be used to reveal patients' private information. Using such data, we explored the patient-doctor interaction patterns. With access to the patients' identifiable information, we recognized the identity of the clients who received internet-based care services and their possible diseases.

Conclusion: This analysis revealed that exposure of patients' confidential information could compromise their identities and underlying medical conditions. This highlights the need for a national framework to ensure the security of health-related electronic data. Health authorities should enforce comprehensive laws, while the owners of televisit websites should implement privacy by design principles into the development of such platforms to prevent the disclosure of sensitive information.

Please cite this article as: Haddad Soleymani M, Mohammadpour A. Assessing Information Confidentiality in Telemedicine Platforms Using Public Web Data: A Case Study of Persian Televisit Websites. Iran J Med Sci. doi: 10.30476/ijms.2025.105205.3899.

Keywords ● Telemedicine ● Electronic health record ● Privacy ● Confidentiality ● Computer security

What's Known

- The growth of telemedicine platforms increases access to healthcare, but raises privacy and confidentiality concerns.
- Electronic Health Records and health-related electronic data are vulnerable to unauthorized access, exposing patients' confidential information.
- Global frameworks such as the Health Insurance Portability and Accountability Act provide guidelines and regulations for protecting health data.
- Iran lacks comprehensive regulations for safeguarding Electronic Health Records and health-related electronic data.

What's New

- Identifying privacy vulnerabilities on Persian televisit websites by analyzing public health-related electronic data.
- Demonstrating how patients' health conditions can be inferred from their televisit patterns.
- Highlighting the lack of robust anonymization of public content on a Persian televisit website.
- Proposing actionable recommendations for regulatory frameworks and data protection practices tailored to Iran's context.

Introduction

The growth in access to computers and smartphones, along with internet connectivity, has initiated the era of digital telelife. In this digital age, most people regularly engage in various online activities, ranging from browsing news headlines and conducting online searches to participating in e-learning courses, engaging in e-commerce, and seeking remote medical consultations. This shift towards a modern, internet-based lifestyle (i-lifestyle) has

generated substantial volumes of electronic data (e-data) in various formats, including unstructured text documents, audio and video files, images, and tabular data. Transferring such e-data over the internet increases its vulnerability to unauthorized access by third-party trackers, highlighting the need for strict supervision. With the rise of the i-lifestyle, the issues of privacy, confidentiality, and security have become more pronounced, particularly regarding personal data. Privacy concerns the right of individuals to control access to private information, including when and how much information to share.[1] Confidentiality relates to data sensitivity, necessitating protection against unauthorized access and disclosure, while security focuses on implementing measures to protect data and prevent unauthorized access.[2]

As part of the shift from traditional in-person doctor visits to internet-based care (i-care) services, several Persian televisit websites have been developed, especially during the COVID-19 pandemic. These platforms offer i-care consultations to anyone with internet access, potentially improving access to healthcare services, increasing care coordination and efficiency, promoting health equity, and reducing healthcare costs. However, using Information Technology (IT) to facilitate i-care services via televisit websites poses various technical and non-technical challenges.[3] A paramount concern is ensuring the confidentiality of patients' information, particularly those stored as Electronic Health Records (EHRs). An EHR is a legal record created and owned by a Care Delivery Organization (CDO), in this case, a televisit website. EHRs are used to document, monitor, and manage the delivery of medical services to patients. They include Patient Identifiable Information (PII) such as name, gender, phone number, and detailed health statuses, including disease background, types of medical services received, and medication details.[4] In addition to such information, televisit websites also contain public health-related e-data such as doctor ratings, service feedback, and general health advice. EHRs and public health-related e-data raise significant concerns about the confidentiality of patients' information. Inappropriate disclosure of such information can jeopardize patients' reputation and life opportunities, fostering hesitancy to seek medical help.[5] Thus, to maintain trust between patients and medical providers, protecting the patients' confidential information from breaches is critical.[6] While privacy and confidentiality are distinct concepts, they are often used interchangeably in the healthcare context. Privacy involves freedom from intrusion, focusing on medical service providers' obligation to shield patients' health data, whereas confidentiality limits information access strictly to authorized people.[2]

Although IT brings many benefits in delivering i-care services, concerns about breaches of confidential information persist. A study in Canada in 2003 revealed that only 25% of organizations had implemented adequate policies and security infrastructures to safeguard information access.[2] Another research highlighted high concerns regarding breaches of confidential information and a lack of control over unauthorized access to such data.[7] Moreover, a study conducted in Emergency Departments (EDs) of Iranian hospitals showed that the patients were dissatisfied with the lack of information privacy.[5] In response to these concerns, strict security measures and regulations are crucial to protect patients' health information. Respecting patients' rights to privacy and confidentiality includes obtaining informed and broad consent before using their personal information for purposes beyond healthcare.[8] Globally, several regulatory frameworks aim to protect health data. For instance, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 in the United States (U.S.) provides regulations for privacy, security, and electronic transactions and outlines penalties for illegal disclosures of health information.[2, 9] Furthermore, HIPAA has provided some regulations on data storage and specific plans to avoid data misuse.[10] Since then, all healthcare providers in the U.S. need to comply with HIPAA to protect patients' information, including any distinct identifying number, their names and characteristics, phone numbers, geographic data, email addresses, Social Security Numbers (SSNs), health records numbers, biometric identifiers (e.g., retinal scans, fingerprints), and full face photos.[10] Other countries have also adopted laws and regulations on protecting health information. In the United Kingdom, the National Health Service (NHS) Code of Practice provides strong guidelines and comprehensive resources on health information security and disclosure to patients, their family members, and legal institutions.[2, 9] Similarly, Australia has policies and a thorough and well-defined legal framework, including laws on health information privacy, which focuses on protecting patients' confidential information while ensuring it can be shared when necessary, e.g., for research purposes.[9, 11] Moreover, Canada's privacy laws and Freedom of Information Law provide guidelines for the Personal Information

Protection and Electronic Documents Act (PIPEDA), which controls and regulates access to health information, ensuring the confidentiality of personal health information.[11]

Despite such frameworks, Iran lacks a unified ethical guideline for the effective protection of patients' confidential information.[6] While there are some formal laws and policies, most regulatory measures in Iran are in the form of guidelines or formal letters. For instance, Chapter Four of the Iranian Patients' Rights Charter states that everyone can demand the rights of privacy and confidentiality.[1] Additionally, Article 648 of Iran's Islamic Penal Code (IPC) states penalties for breaching confidential information except for legally justified disclosures, and the Disciplinary Regulation of Iran's Medical Council (DRIMC) forbids the breach of confidential information.[6] Some other general regulations on the disclosure of EHRs apply to patients. Still, no clear guidelines exist for their family members or for purposes such as research or sharing data with insurance companies.[9]

In addition to the need to establish the necessary laws, the owners of the televisit websites have to prioritize the confidentiality of patients' information. They have to use appropriate safeguards to protect individuals from discrimination or stigmatization related to their health statuses. To keep individuals' information safe, the owners of such websites should follow data confidentiality rules and guidelines on how basic ethical principles and necessities should direct or constrain their decisions and actions. They should preserve patients' confidential information and consider how its release could harm their well-being. Recent advancements in data protection technologies, such as anonymization and encryption, offer promising methods for preserving information confidentiality. Anonymization is a method for safeguarding individuals from being recognized. ISO defines it as removing the links between identifiable data and the data subject.[12] The developers of televisit websites are encouraged to rigorously implement such de-identification methods to prevent disclosure of confidential information.

Despite the rapid growth of Persian televisit websites, there has been little empirical research on how public web data on such websites might unintentionally disclose patients' private information. This study demonstrates how it was possible to infer the patients' private information using only public health-related e-data on a televisit website. Specifically, it explores how such data can be used to reveal patients' identities and their possible diseases.

Materials and Methods

This section outlines the method used in this observational case study. We collected PII and other health-related e-data by scraping a Persian televisit website—without engaging in illegal activities such as hacking—to reveal patients' identities and their potential diseases. In this paper, the terms "scrap", "harvest", and "extract" are used interchangeably to describe the process of collecting web data for analysis.

We focused on harvesting data on two main entities: the patients and the doctors they consulted *via* televisit. Data harvesting and preparation were primarily conducted using SAS 9.4 software (SAS Institute Inc., Cary, NC, USA). It provided robust procedures (procs), functions, call routines, and macro capabilities essential for harvesting, cleaning, and transforming messy data—the data that were disorganized or poorly structured. Microsoft Excel 2019 (Microsoft Corporation, Redmond, WA, U.S.) and RStudio 2022.02.0 (Integrated Development Environment for R, originally developed at the University of Auckland, New Zealand) software programs were additionally employed for data visualization.

Our work followed these main steps:

1. Data Extraction (E phase): Initially, we extracted messy and unstructured data from the target website during the extraction phase. This involved connecting to the website's Uniform Resource Locator (URL) using PROC HTTP and employing Perl Regular Expression (PRX) to fetch selective information based on defined text patterns.

2. Data Transformation (T phase): The raw data were then transformed into structured datasets during this phase. We utilized PROC SQL for efficient data management and transformation, ensuring the data were well-organized and suitable for analysis.

3. Data Loading (L phase): In this phase, the structured datasets were loaded into a SAS software library, being prepared for integration and further analysis.

4. Data Integration and Preparation: We integrated datasets prepared in the previous step into a structured multiple-rows-per-patient dataset. Then, the required features were computed, facilitating a detailed analysis of the interaction between the patients and the doctors.

5. Data Analysis: The final step involved analyzing the data using several software programs. Microsoft Excel software program was utilized to create Treemap charts, and the networkD3 library in the RStudio software program was employed to create a Sankey

diagram that visualizes the patient-doctor relationship and the televisit patterns.

This multi-software approach enabled a thorough examination of the harvested data, ensuring robust insights into the information confidentiality concerns associated with televisit websites. Given the dynamic nature of websites and to ensure data consistency, all data were extracted in a session on March 16, 2022. It is worth mentioning that the Extract, Transform, Load (ETL) process took 19,860 seconds (5 hours and 31 min) to execute.

As part of our data collection, we accurately extracted and stored information about patients and the doctors they had televisited into separate SAS software datasets. Specifically, from the target website, we scraped web pages for PII, including the patients' full names and phone numbers. Doctors' information was obtained from two different web pages: one containing doctors' full names and another detailing their specialties. Figure 1 represents the Entity Relationship Diagram (ERD), illustrating the data structure of the datasets and the relationship between them. The ERD depicts the relationship between the doctor and specialty datasets as one-to-zero-or-one, indicating that some of the doctors did not declare their specialty at the time of data harvesting. The relationship between the doctor and the patient datasets is defined as one-to-zero-or-many, reflecting that a doctor may have provided i-care services to multiple patients, or none, as recorded.

Merging these datasets and rolling up over the "time_of_televisit" and "date_of_televisit" features resulted in a multiple-rows-per-patient dataset consisting of 392 rows and nine features. As illustrated in table 1, each row encapsulates the interactions between the patients and the doctors, detailing the number of televisits made. Table 1 documents that the patient identified as 5338…4CE9 had five televisits on the target website. This patient got three and two televisits from doctors identified with the IDs 0102…7707 and AD1E…8EC6, respectively. The feature "Doctor Total Televisits" quantifies the total number of televisits made by each doctor. For

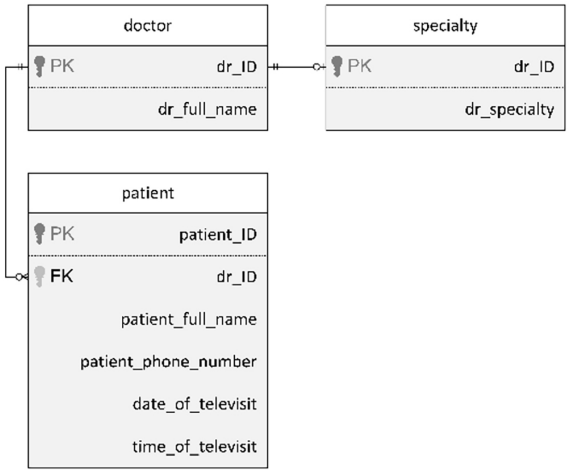

Figure 1: The Entity relationship diagram shows the structure of and the relationship between the doctor, the specialty, and the patient datasets.

instance, the doctor identified as 0102…7707 made eight televisits, while the doctor with the encoded ID AD1E…8EC6 made six, as recorded on the target website. It should be noted that, as the data harvested from the target website were accessible to the public, our study did not require any informed consent or ethical approval. However, it is essential to handle such data responsibly and by ethical standards to ensure the protection of sensitive information and to prevent the identification of individuals involved. Thus, we applied a hashing algorithm to encode the personal information of the patients and the doctors.

The subsequent section will describe how we utilized this aggregated information to infer and disclose the patients' medical conditions, illustrating the potential privacy implications and the effectiveness of our data-handling method.

Results

This section is organized into two main parts. Adhering to best practices, we first described the final dataset to establish a foundational understanding before applying any analytical techniques. Next, we detailed how the data had been analyzed to reveal patients' possible diseases.

Table 1: The structure of the final dataset

Patient ID	Patient Full Name	Patient Phone Number	Doctor ID	Doctor Full Name	Specialty	Patient Total Televisits	Patient-Doctor Televisits	Doctor Total Televisits
5338...4CE9	6637…140D	B8B7...5CCA	0102…7707	7AE3…DDFE	4799…4653	5	3	8
5338...4CE9	6637…140D	B8B7...5CCA	AD1E…8EC6	1DF6…87D3	4207…16FE	5	2	6
492B…373A	5172…58C3	5D60…E310	A0C8…F3E4	3960…D001	4D78…9DF6	5	2	2
492B…373A	5172…58C3	5D60…E310	0102…7707	7AE3…DDFE	4799…4653	5	1	8
492B…373A	5172…58C3	5D60…E310	E95C…3BC0	1C3C…8862	6EA2…37F5	5	1	2
492B…373A	5172…58C3	5D60…E310	E8AB…5FAB	54A9…D7C9	2A30…A035	5	1	5

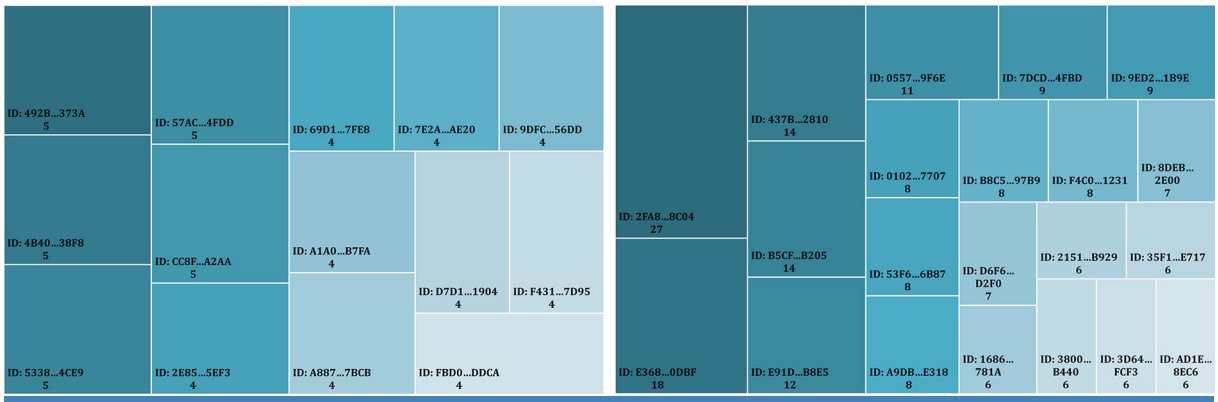

Figure 2: The Treemap charts illustrate that the patients received four or more televisits (left) and the doctors made six or more televisits (right) on the target website, represented by their encoded IDs

Data Description

The final dataset includes multiple entries per patient, amounting to 392 rows and nine features. This dataset encapsulates information about 263 patients and 194 doctors, as captured from the target website. The left-hand panel of figure 2 displays a Treemap chart highlighting the patients engaged in four or more televisits, showing that the maximum recorded number of televisits a patient received was five. The right-hand panel of figure 2 illustrates a Treemap chart for the doctors who made six or more televisits, indicating that the highest number of televisits made by a doctor on the target website was 27.

Disclosure of Patients' Possible Diseases

The primary focus of this study involved a detailed examination of how harvested public web data were utilized to infer and disclose patients' potential diseases. This analysis assumes that patients rationally consult specialists relevant to their health conditions, e.g., someone with an eye condition would logically visit an optometrist or ophthalmologist rather than an orthopedic surgeon or an Ear, Nose, and Throat (ENT) specialist.

We could deduce patients' possible diseases by analyzing the patterns related to their televisits on the target website. This process, while revealing data analysis capabilities, raised significant privacy concerns. Access to PII made it possible to recognize patients' identities, posing a serious privacy violation and disclosure of confidential information.

To illustrate our analysis method, we initially demonstrated how the patients and the doctors were connected on the target website. Figure 3 illustrates a Sankey diagram used to show the relationship between the patients and the doctors for the patients who received more than two televisits. In the diagram, the encoded patients' IDs are positioned on the left, and the encoded doctors' IDs appear on the right. It provides a clear visual pathway of the patient-doctor relationship without revealing actual identities. The thickness of the gray lines corresponds to the frequency of televisits as quantified by the "Patient-Doctor Televisits" feature. This visual presentation is instrumental in identifying the patterns related to the patients' televisits to the specific doctors.

To further clarify our method and confirm the results, we include selected rows and features from the final dataset in table 2, showing the "Specialty" feature before encoding. The inclusion of the "Specialty" feature before encoding provides a transparent view into how effectively our method could deduce the patients' possible diseases from their televisit patterns.

Table 2 provides encoded data, except for the "Specialty" feature, illustrating how the patients' televisits to the specific doctors can suggest underlying health concerns:

- The patient B2DB…2711, frequently televisited an obstetrician-gynecologist and ultrasound and radiology specialists, suggesting a woman having gynecological or maternal health concerns.
- The patient A002…71C1 registered multiple televisits to a urologist and ultrasound and radiology specialists, indicating this client may have potential urinary system issues.
- Televisit patterns of the patient 066A…FB71, twice to a pediatrician and once to a pediatric nephrologist, suggest this client may be a child who suffers from a urinary system condition.

By analyzing the patterns related to patients' televisits on the target website, we revealed potential diseases based on the data collected at that time. Access to PII enhances our ability to identify specific individuals, raising significant concerns about privacy and confidentiality. Therefore, it is crucial to protect such sensitive information from public access to maintain the patients' confidential information and prevent unauthorized disclosure.

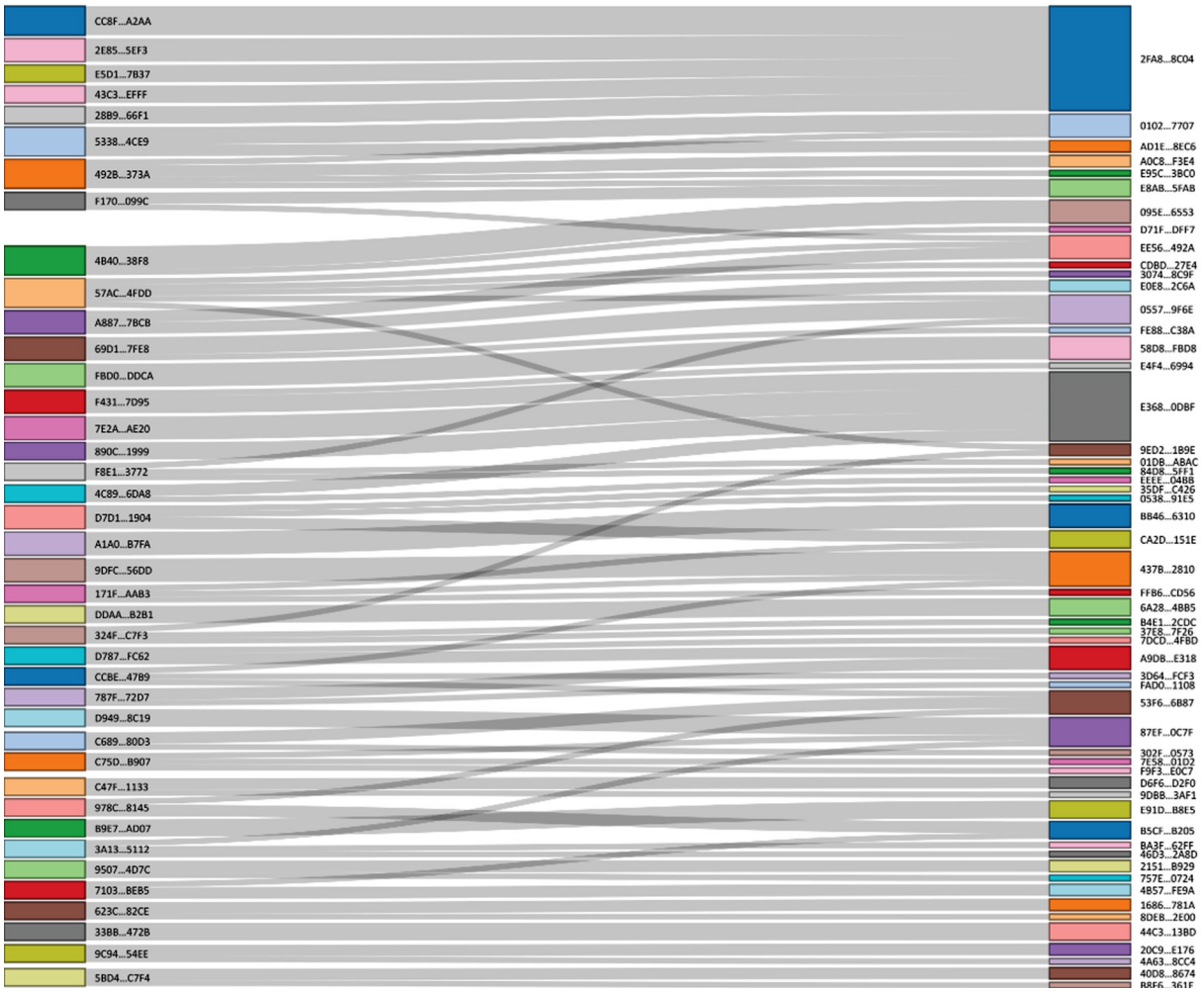

Figure 3: The Sankey diagram demonstrates the relationship between the patients (left) and the doctors (right), represented by their encoded IDs and the frequency of televisits (thickness of the gray lines) for the patients who received more than two televisits.

Table 2: Selected rows from the final dataset with the specialty feature before encoding

Patient ID	Patient Full Name	Patient Phone Number	Doctor ID	Specialty	Patient Total Televisits	Patient-Doctor Televisits
57AC…4FDD	B2DB…2711	5155…5E74	CDBD…27E4	Pathologist	5	1
57AC…4FDD	B2DB…2711	5155…5E74	EE56…492A	Ultrasound Specialist and Radiologist	5	1
57AC…4FDD	B2DB…2711	5155…5E74	3074…8C9F	Radiologist	5	1
57AC…4FDD	B2DB…2711	5155…5E74	0557…9F6E	Obstetricians and Gynecologists	5	1
57AC…4FDD	B2DB…2711	5155…5E74	9ED2…1B9E	Ultrasound Specialist and Radiologist	5	1
F170…099C	A002…71C1	779C…1C68	E8AB…5FAB	Urologist	3	2
F170…099C	A002…71C1	779C…1C68	EE56…492A	Ultrasound Specialist and Radiologist	3	1
C47F…1133	066A…FB71	258C…159C	D6F6…D2F0	Pediatrician	3	2
C47F…1133	066A…FB71	258C…159C	9DBB…3AF1	Pediatric Nephrologist	3	1

Discussion

This study revealed that it is possible to infer potential diseases of patients from public health-related e-data on a Persian televisit website, without the need for hacking or illegal access. By tracking the patients' televisit patterns and using their PII, we identified vulnerabilities in information confidentiality on the target website. Our results highlighted that even non-sensitive-looking information can be employed to disclose private personal information. This aligns with findings from similar studies in other countries, which have shown that health-related e-data can inadvertently reveal sensitive information when not adequately anonymized. Our findings illustrate how disclosure of private information can occur on poorly developed televisit websites, even in the absence of direct malicious intent.

The rapid increase in telemedicine platforms during the COVID-19 pandemic has significantly transformed the delivery of i-care services. The increase in the development of Persian televisit websites, paralleled by the rise in internet users, has notably enhanced healthcare accessibility. However, this shift raises crucial questions about the confidentiality of EHRs compared to paper-based health records.[13] Televisit websites generate vast amounts of health-related e-data recognized as "big data", characterized by their volume, velocity, veracity, and variety. The transmission of such e-data over the internet intensifies concerns around information privacy and confidentiality, as it opens opportunities for third-party trackers to misuse personal information for marketing, financial gain, or even extortion.

Ensuring the confidentiality of information must go beyond securing internal databases to include the protection of public web data as well. Our study provides a concrete example of how inadequate handling of health-related e-data can lead to unintentional disclosure of patients' health information, reinforcing the urgent need for stronger regulatory oversight, technical safeguards, and the importance of Privacy by Design (PbD) principles. Thus, ensuring the confidentiality of patients' information has emerged as a paramount issue. To safeguard such e-data, health regulatory authorities are urged to develop and enforce comprehensive laws and policies governing telemedicine platforms. Despite rigorous efforts to protect information confidentiality, the inherent vulnerabilities of televisit websites pose ongoing threats. Addressing these threats necessitates a multidisciplinary approach involving multiple stakeholders.[14]

In Iran, where the regulatory landscape for EHRs and public health-related e-data is still nascent, there is a pressing need for more robust rules and guidelines, especially to protect such e-data from unauthorized access.[2] Although national policies are still in their formative stages, the adoption of global standards, such as those proposed by HIPAA or the World Health Organization (WHO), is crucial.[15] These standards emphasize patients' safety, privacy, and the ethical management of sensitive information, recommending measures such as patients' informed consent before data sharing, rigorous data encryption, and system access controls to prevent information breaches.[15] Although Iran has adopted some general legal frameworks, such as the Electronic Commerce Law, which helps transfer data securely via systems, we need comprehensive and specific laws on accessing EHRs and public health-related e-data.[11] Iranian medical and health service providers have limited internal policies that need to distinguish between paper-based health records and EHRs, leading to inconsistencies in their application.[11]

To the best of our knowledge, this study is the first to illustrate how public health-related e-data on a Persian televisit website can easily, even without malicious intent or hacking, reveal the patients' identities and their possible diseases. This vulnerability highlights the necessity and the importance of integrating PbD principles into the development and maintenance of televisit websites. Before launching a televisit website, it is critical to address the security of the website's public content to ensure robust legal frameworks are in place and to confirm that the sharing of patients' public health-related e-data is reliant on their informed consent.

As mentioned earlier, this study was conducted using public health-related e-data. Nevertheless, the most important limitation of our study is that it was not possible to evaluate all Persian televisit websites to find out if there have been other cases of confidentiality leakage. Additionally, the large volume of such data made the scraping process too difficult and time-consuming.

Conclusion

This observational case study revealed that public health-related e-data on a Persian televisit website could be used to identify the patients and infer their possible diseases. Notably, this exposure occurred without any unauthorized access or technical exploitation, highlighting how seemingly benign public health-related e-data, when cross-referenced, can lead to serious breaches of patients' confidential information. The findings demonstrate a significant privacy risk inherent in such telemedicine platforms that lack proper data anonymization and protection protocols.

We advocate for developing and implementing a thorough national framework by the Ministry of Health and Medical Education (MoHME) in collaboration with IT experts and medical professionals. This framework should be tailored to meet Iran's exclusive requirements and include:

- Clear regulations on how to access and publish web data, specifically health-related e-data.
- Adherence to security protocols and health ethics to prevent breaches of confidential information.
- Implementation of advanced anonymization and de-identification techniques.
- Patients' rights to ensure they are informed

of how their health-related e-data are being used.

Additionally, the owners of the televisit websites should adopt up-to-date techniques and technologies to effectively de-identify their clients' information. Utilizing robust hashing algorithms to obscure PII can protect patients' confidential information even if third-party trackers access it. Moreover, patients need to be aware of their rights in case their information is compromised.

To further our efforts in safeguarding patients' information on televisit websites, we propose the following areas for future research:

• Assessment of Persian televisit websites to identify other instances of confidential information leakage.

• Development of solutions to prevent unauthorized access to EHRs and health-related e-data.

• Increasing patients' awareness of their rights in case their health-related e-data have been published or used without informed consent.

Authors' Contribution

M.HS.: Study design, data extraction, analysis, drafting, and reviewing the manuscript; A.M.: Data analysis and reviewing the manuscript. All authors have read and approved the final manuscript and agree to be accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work are appropriately investigated and resolved.

Conflict of Interest: None declared.

References

1 Mohammadi M, Larijani B, Emami Razavi SH, Fotouhi A, Ghaderi A, Madani SJ, et al. Do patients know that physicians should be confidential? study on patients' awareness of privacy and confidentiality. J Med Ethics Hist Med. 2018;11:1. PubMed PMID: 30258551; PubMed Central PMCID: PMCPMC6150920.

2 Basil NN, Ambe S, Ekhator C, Fonkem E. Health Records Database and Inherent Security Concerns: A Review of the Literature. Cureus. 2022;14:e30168. doi: 10.7759/cureus.30168. PubMed PMID: 36397924; PubMed Central PMCID: PMCPMC9647912.

3 Eslami Jahromi M, Ayatollahi H. Utilization of telehealth to manage the Covid-19 pandemic in low- and middle-income countries: a scoping review. J Am Med Inform Assoc. 2023;30:738-51. doi: 10.1093/jamia/ocac250. PubMed PMID: 36565464; PubMed Central PMCID: PMCPMC10018263.

4 Chishtie J, Sapiro N, Wiebe N, Rabatach L, Lorenzetti D, Leung AA, et al. Use of Epic Electronic Health Record System for Health Care Research: Scoping Review. J Med Internet Res. 2023;25:e51003. doi: 10.2196/51003. PubMed PMID: 38100185; PubMed Central PMCID: PMCPMC10757236.

5 Mobasher M, Samzadeh Kermani H, Eslami Shahrbabaki M, Sarafinejad A. Study of Patients' Privacy during the COVID-19 Pandemic in Iranian Health Care Settings. Iran J Med Sci. 2024;49:580-9. doi: 10.30476/ijms.2023.97795.3070. PubMed PMID: 39371378; PubMed Central PMCID: PMCPMC11452588.

6 Noroozi M, Zahedi L, Bathaei FS, Salari P. Challenges of Confidentiality in Clinical Settings: Compilation of an Ethical Guideline. Iran J Public Health. 2018;47:875-83. PubMed PMID: 30087874; PubMed Central PMCID: PMCPMC6077627.

7 Ayatollahi H, Mirani N, Haghani H. Electronic health records: what are the most important barriers? Perspect Health Inf Manag. 2014;11:1c. PubMed PMID: 25593569; PubMed Central PMCID: PMCPMC4272437.

8 Langarizadeh M, Moghbeli F, Aliabadi A. Application of Ethics for Providing Telemedicine Services and Information Technology. Med Arch. 2017;71:351-5. doi: 10.5455/medarh.2017.71.351-355. PubMed PMID: 29284905; PubMed Central PMCID: PMCPMC5723167.

9 Ammenwerth E, Duftschmid G, Al-Hamdan Z, Bawadi H, Cheung NT, Cho KH, et al. International Comparison of Six Basic eHealth Indicators Across 14 Countries: An eHealth Benchmarking Study. Methods Inf Med. 2020;59:e46-e63. doi: 10.1055/s-0040-1715796. PubMed PMID: 33207386; PubMed Central PMCID: PMCPMC7728164.

10 Theodos K, Sittig S. Health Information Privacy Laws in the Digital Age: HIPAA Doesn't Apply. Perspect Health Inf Manag. 2021;18:1l. PubMed PMID: 33633522; PubMed Central PMCID: PMCPMC7883355.

11 Tavakoli N, Isfahani SS, Piri Z, Amini A. Patient access to electronic health record: a comparative study on laws, policies and procedures in selected countries. Med Arch. 2013;67:63-7. doi: 10.5455/medarh.2013.67.63-67. PubMed PMID: 23678844.

12 Langarizadeh M, Orooji A, Sheikhtaheri A. Effectiveness of Anonymization Methods in Preserving Patients' Privacy: A Systematic Literature Review. Stud Health Technol

Inform. 2018;248:80-7. PubMed PMID: 29726422.
13 Carlson JL, Goldstein R. Using the Electronic Health Record to Conduct Adolescent Telehealth Visits in the Time of COVID-19. J Adolesc Health. 2020;67:157-8. doi: 10.1016/j.jadohealth.2020.05.022. PubMed PMID: 32517972; PubMed Central PMCID: PMCPMC7275171.
14 Jalali MS, Landman A, Gordon WJ. Telemedicine, privacy, and information security in the age of COVID-19. J Am Med Inform Assoc. 2021;28:671-2. doi: 10.1093/jamia/ocaa310. PubMed PMID: 33325533; PubMed Central PMCID: PMCPMC7798938.
15 Abedian S, Riazi H. E-Health: Security, Privacy, and Ethics Requirements from a National Perspective in I. R. Iran. Stud Health Technol Inform. 2024;314:147-8. doi: 10.3233/SHTI240079. PubMed PMID: 38785021.