Risk Management and Healthcare Policy

Dovepress
open access to scientific and medical research

Open Access Full Text Article

ORIGINAL RESEARCH

Security Risk Assessment for Patient Portals of Hospitals: A Case Study of Taiwan

Pei-Cheng Yeh[1,2], Kuen-Wei Yeh[3–5], Jiun-Lang Huang[6,7]

[1]Graduate Institute of Clinical Dentistry, School of Dentistry, College of Medicine, National Taiwan University, Taipei, Taiwan, Republic of China; [2]Division of Endodontics, Department of Stomatology, Taichung Veterans General Hospital, Taichung, Taiwan, Republic of China; [3]Investigation Bureau, Ministry of Justice, New Taipei City, Taiwan, Republic of China; [4]Department of Electrical Engineering, Chinese Culture University, Taipei, Taiwan, Republic of China; [5]Department of Information, Chinese Culture University, Taipei, Taiwan, Republic of China; [6]Department of Electrical Engineering, National Taiwan University, Taipei, Taiwan, Republic of China; [7]Graduate Institute of Electronics Engineering, National Taiwan University, Taipei, Taiwan, Republic of China

Correspondence: Kuen-Wei Yeh, Email m49009@mjib.gov.tw

Background: Growing cyberattacks have made it more challenging to maintain healthcare information system (HIS) security in medical institutes, especially for hospitals that provide patient portals to access patient information, such as electronic health record (EHR).

Objective: This work aims to evaluate the patient portal security risk of Taiwan's EEC (EMR Exchange Center) member hospitals and analyze the association between patient portal security, hospital location, contract category and hospital type.

Methods: We first collected the basic information of EEC member hospitals, including hospital location, contract category and hospital type. Then, the patient portal security of individual hospitals was evaluated by a well-known vulnerability scanner, UPGUARD, to assess website if vulnerable to high-level attacks such as denial of service attacks or ransomware attacks. Based on their UPSCAN scores, hospitals were classified into four security ratings: absolute low risk, low to medium risk, medium to high risk and high risk. Finally, the associations between security rating, contract category and hospital type were analyzed using chi-square tests.

Results: We surveyed a total of 373 EEC member hospitals. Among them, 20 hospital patient portals were rated as "absolute low risk", 104 hospital patient portals as "low to medium risk", 99 hospital patient portals as "medium to high risk" and 150 hospital patient portals as "high risk". Further investigation revealed that the patient portal security of EEC member hospitals was significantly associated with the contract category and hospital type ($P<0.001$).

Conclusion: The analysis results showed that large-scale hospitals generally had higher security levels, implying that the security of low-tier and small-scale hospitals may warrant reinforcement or strengthening. We suggest that hospitals should pay attention to the security risk assessment of their patient portals to preserve patient information privacy.

Keywords: security risk assessment, healthcare information system, electronic health record, electronic medical record, EMR Exchange Center, vulnerability scanner

Introduction

Patient information privacy has emerged as a critical issue in recent years.[1–3] Large volumes of potentially sensitive patient information, such as name, ID, birth date, contact phone and health record, are preserved in medical institutes. The electronic health record (EHR)[1–7] is a digital version of the traditional paper-based personal health record. Using EHR, personal health records can be accessed with online services and shared between hospitals and patients. A healthcare information system (HIS)[1–3] refers to a system designed to manage and utilize patient information. In general, HIS consists of internal physician systems and external patient portal. Physician systems are designed to support medical diagnosis and treatment of healthcare professionals. The doctors can trace patient medical records through physician systems. Due to safety considerations, physician systems are only for internal use and disable connections from the Internet. Compared to physician systems, patient portals[3–6] are utilized to serve hospital patients. The main purpose of patient portals is to give patients easy access to their medical records to enhance patient engagement. Patient portals are web-based platforms or mobile APPs to offer online reservations, in-time consultation, patient data maintenance and

Received: 7 February 2024
Accepted: 29 May 2024
Published: 18 June 2024

instant EHR search. To obtain permission to use patient portals, patients should apply for a portal account from the hospital. If the application is approved, the hospital will assign one unique portal account to patients for portal login. Figure 1 shows an example of a patient portal in Taiwan. When patients visit the patient portal website via the Internet, the website will redirect to its login page and ask patients to enter the correct portal account and password to gain authorized access (block 1). If login is successful (block 2), the website will redirect patients to their personal main pages (block 3), which are often called "My Health Bank". In personal main page, patients can search for personal medical records, pharma records, registration inquiries and maintain personal data. In addition to individual portal accounts, most patient portals have administrator accounts, which are utilized by system admins to maintain patient portals. The administrator accounts are permitted to use high-priority functions, such as querying any patient information for the purpose of patient management or system problem solving. In addition, EHR exchange has become a major trend to reduce unnecessary treatments for patients and enhance the EHR interoperability between hospitals. In 2009, Taiwan's Ministry of Health and Welfare (MOHW) established the EMR Exchange Center (EEC) to operate a cross-hospital HIS for EMR (Electronic Medical Record) exchange.[7] Currently, EEC involves 404 member hospitals (including public and private hospitals) and 5872 clinics. Figure 2 shows the architecture of EMR exchange in Taiwan. Member hospitals and clinics connect to EEC via NHI-VPN (National Health Insurance-Virtual Private Network) and exchange EMR by gateway servers. The standardized medical records, uploaded by HIS, were stored in the gateway for EMR exchange. For example, when hospital A request for EMR of hospital B, the request will be first sent to EEC through gateway A (block

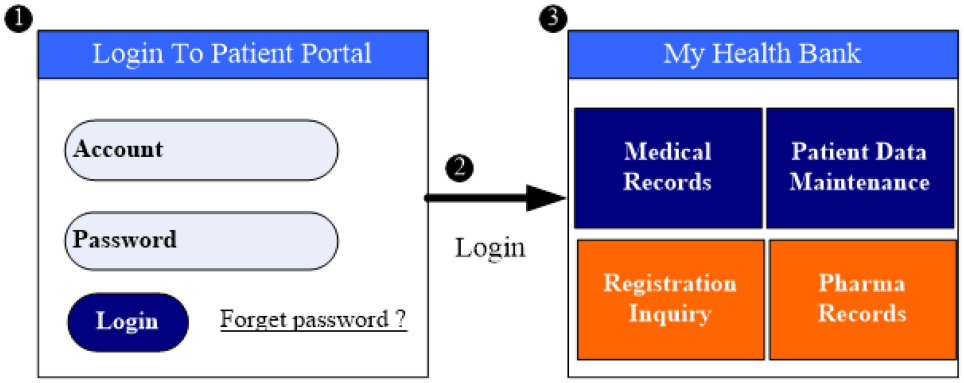

Figure 1 Flow diagram of the patient portal login.

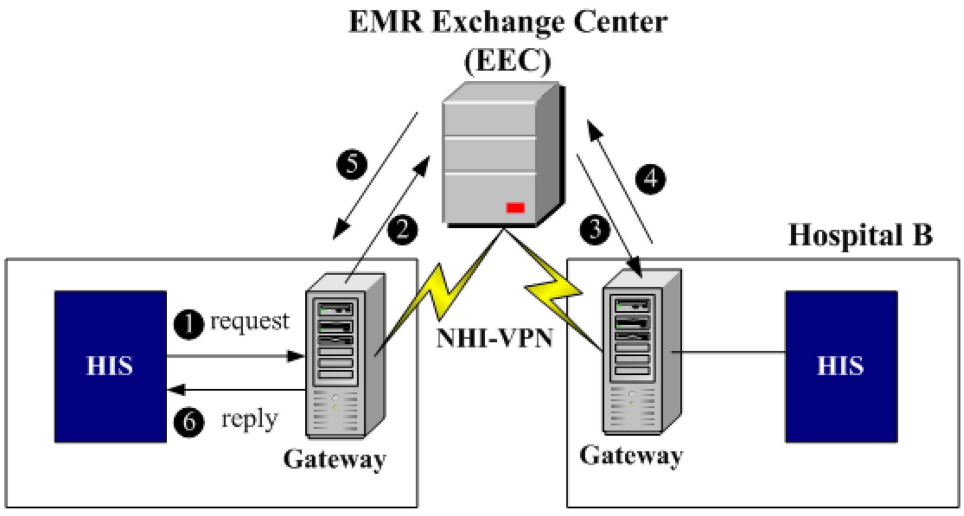

Figure 2 Flow diagram of EMR exchange.

1 and 2). Second, EEC transfers the request to hospital B through gateway B (block 3). Third, gateway B responds EMR to EEC (block 4). Finally, EEC returns EMR to hospital A (block 5 and 6). In addition, to avoid repetitive EMR exchange, the request hospital is permitted to store replied EMR of other hospitals under patient agreement for future use.

Compared to physician systems, patient portal security risk is emerging as a new challenge for HIS due to the growing cyber threats.[6–14] Cyber threat is the collection of criminal activities that use computers to issue cyberattacks through the Internet. Hacking[8,14–17] is one of the common forms of cyberattacks, aiming to crack information systems so as to gain unauthorized identity to steal data or encrypt user files to extort money. The basic concept of hacking is to find and exploit the information system weakness. Hackers, who engage in hacking, are generally divided into two types – black hat hacker and ethical hacker (white hat). Black hat hackers engage in hacking for malicious purposes, for example, to gain illegal benefits by selling the stolen data.[16–18] Because of the huge benefit of hacking, more and more people are involved in this underworld activity. Black hat hackers can take advantage of hospital's patient portal weakness for their illegal benefits. For example, the 2020 cyber security report of MOHW[19] reported that EEC suffered serious hacking on August 29,2019 — a total of 38 member hospitals (maybe up to 66, unverified) were infected by ransomware.[20–22] Further inspection revealed that there are weaknesses in the patient portal of a number of EEC member hospitals. This event showed that medical institutes have been targeted by black hat hackers for cracking; as a result, patient portal security of hospitals is worthy of investigation and should be considered into risk assessment.

The existence of website weakness[11,23–26] is the cause of patient portal hacking. One of the common website weaknesses is human carelessness, with weak passwords[27] being the most notorious. It is common that system administrators or patients use often-seen or short strings as their passwords. These weak passwords are easily guessable or suffer from brute-force attacks. Especially when administrator accounts are leaked, not only individual patients, whole database can be stolen. Another common website weakness is the design loophole, which is poor website design that black hat hackers can exploit to crack the website.

Background

Security risk assessment[25,28,29] is a process that aims to identify potential threats and vulnerabilities to business assets, and analyze the impact and likelihood of each threat. To prevent hacking, it is crucial to perform security risk assessment for patient portals before being exploited by black hat hackers. There are a few known frameworks proposed for security risk assessment, such as NIST Cybersecurity Framework[30] and OWASP,[28,31] providing guidelines on how to identify and evaluate cybersecurity risks. To identify potential threats and vulnerabilities, several vulnerability scanners,[25,28,31] computer tools are available to test computers, networks or applications automatically for known weaknesses. Once identified, these weaknesses can be fixed by system designers. Diagnosis results reported by vulnerability scanners also indicate the level of website security.

Due to the representativeness and the importance of EEC member hospitals in Taiwan medical institutes, this paper aims to investigate the patient portal security of Taiwan's EEC member hospitals, justify the introduced impact factors of patient portal security with statistical analyses and identify the common weaknesses of patient portals. This survey was conducted in 2022.

Methods

Data Source

To estimate the EEC patient portal security rating, we analyzed the basic information of its member hospitals collected from MOHW. The information included the hospital name, type, location, and contract category. Depending on the contract category they belong to, these medical institutions are classified, according to the hierarchy of medical care in Taiwan, into medical centers, regional hospitals, district hospitals and clinics. However, clinics were later excluded from our analyses because most of them had no patient portals; thus, lack of samples for analysis.

The hospital type, another important classification criterion, consists of general hospitals, ordinary hospitals, and other hospitals (including specialty hospitals, psychiatric hospitals and chronic hospitals). According to MOHW's definition, general hospitals are those containing more than six departments of medical services including internal

medicine, surgery, pediatrics, obstetrics and gynecology, anesthesiology, radiology and others. Furthermore, each department should have specialist physicians and more than 100 hospital beds. Ordinary hospitals are institutions with one or more departments of medical operations with each department having specialist physicians. Compared to ordinary hospitals and other hospitals, general hospitals offer more integrated medical services. The hospital location shows the local government where hospitals are located. There are three types of local government, including municipality, county and city, in Taiwan.

Upguard Overview

UPGUARD (2022 UpGuard, Inc.)[32] is a simple and popular vulnerability scanner that scans and evaluates the security rating of the given website. The UPGUARD contains multiple vulnerability checks. The security rating algorithm is subtractive, starting with a score of 950 and have points subtracted for each vulnerability check they fail. The number of points deducted is based on the impact and probability of that vulnerability being exploited, which was assessed by the industry best security risk assessment frameworks, such as NIST Cybersecurity Framework[30] and OWASP,[28,31] to ensure reliability and validity. Thus, the resulting scores range from 0 to 950, with higher scores indicating less found risk and implying better security. UPGUARD then evaluates websites with resulting score and defines four security ratings as "absolute low risk" (score ranges from 801 to 950, representing for absolute low risk for a data breach in the immediate future), "low to medium risk" (score ranges from 601 to 800, representing for low to medium risk of a data breach in the immediate future), "medium to high risk" (score ranges from 401 to 600, representing for medium to high risk of a data breach in the immediate future) and "high risk" (score below 400, representing for high risk of being breached in the immediate future). An illustrative example of the security rating flow is depicted in Figure 3. In the example, UPGUARD contains N vulnerability checks and the weighting of each vulnerability check i is w_i (block 1). Suppose the target patient

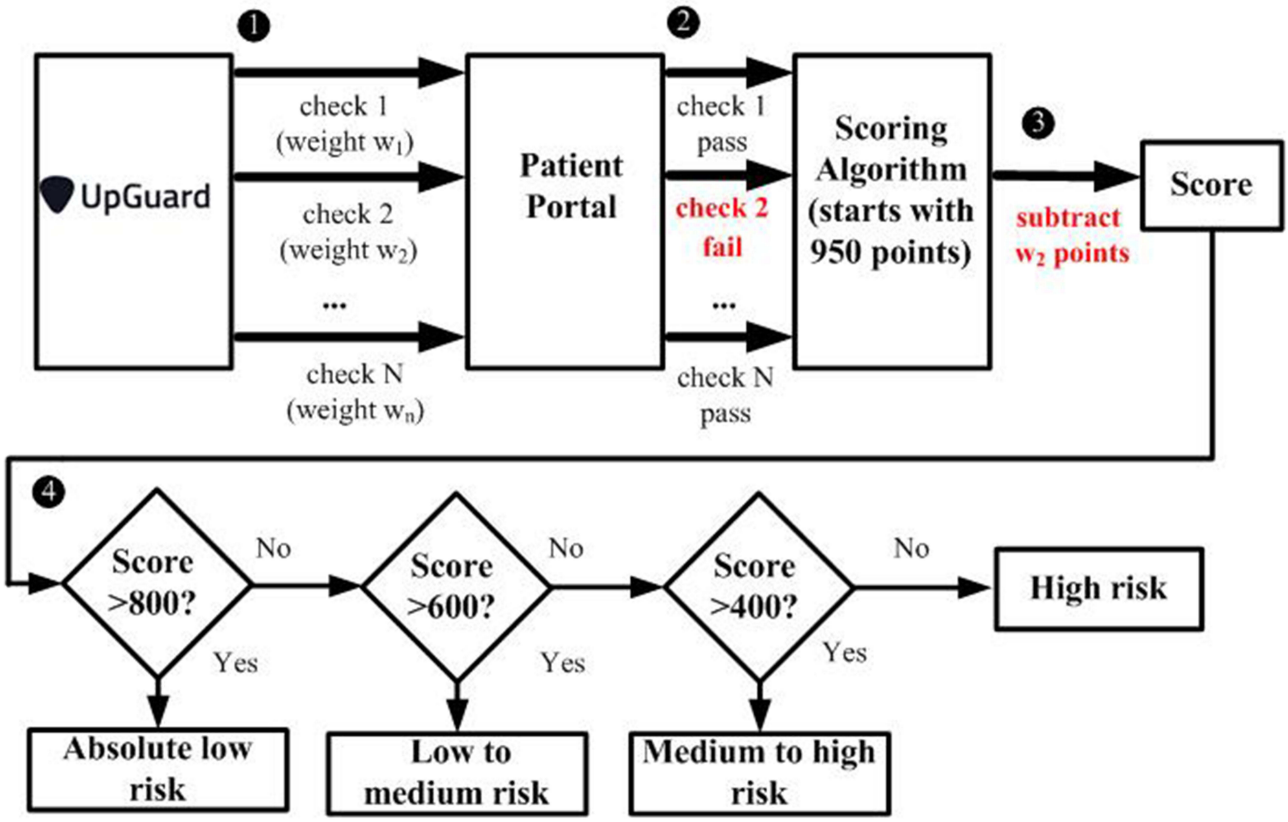

Figure 3 Flow diagram of UPGUARD security rating.
Note: In Figure 3, the symbol *** means ellipsis. For example, we used check1, check2 *** check N to represent for all of *N* checks.

portal fails to pass vulnerability check 2 (block 2), w2 points will be subtracted from the scoring algorithm (block 3). The patient portal security rating will be finally evaluated based on the resulting score of the scoring algorithm (block 4).

Definition

To evaluate patient portal security, we scanned the website security for hospital patient portals. The security of mobile apps accessing patient portals was excluded from our survey. In addition, our study focused on the patient portal security of EEC member hospitals because they are involved in EMR exchange and prone to be cyberattack target. The security of patient portals was determined with the security rating evaluated by UPGUARD.

Study Design

The flow diagram for evaluating the patient portal security of EEC member hospitals is shown in Figure 4. First, we downloaded the list of EEC member hospitals from MOHW. Among them, medical centers, regional hospitals, district hospitals (a total of 404) were selected for further analysis (block 1). Second, we located their patient portals on Google (block 2), and found a total of 373 patient portals. We excluded 31 hospitals because no patient portal could be found. The websites were scanned, scored and evaluated by UPGUAD (block 3). Finally, statistical analyses were performed to identify the relationship between the website security rating of the EEC member hospitals and the following factors: hospital location, contracted category and hospital type (block 4).

Statistical Analyses

We analyzed four categorical variables: security rating, hospital location, contracted category and hospital type. Among them, the security rating variable is the defined variable that has four possible values —absolute low risk, low to medium risk, medium to high risk and high risk corresponding to the security rating by UPGUARD. We used the chi-square test to determine the statistical differences between categorical variables. Statistical significance was set at $P<0.05$.

Ethical Considerations

This research is part of an investigation into EEC hospitals ransomware hacking issue that happened in Taiwan, 2019.[19] The corresponding author, KW Yeh, works for the Investigation Bureau and Ministry of Justice (MJIB) and gets permission to investigate the hacking issue, including if there are weaknesses in the websites of EEC member hospitals. In addition, only non-intrusive vulnerability scanner is utilized to test websites in this research. There is no interference with the functionality of hospital websites.

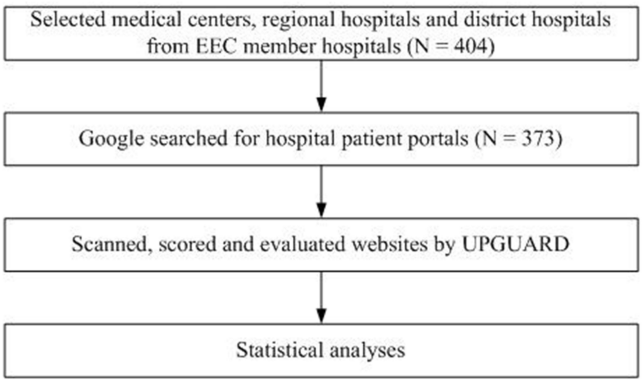

Figure 4 Flow diagram of the study design.

Results

Data from a total of 373 EEC member hospitals were analyzed. The comparison between security rating, contracted category, hospital type and location is shown in Table 1. We found 20 hospital patient portals with "absolute low risk" security rating, 104 hospital patient portals with "low to medium risk" security rating, 99 hospital patient portals with "medium to high risk" security rating and 150 hospital patient portals with "high risk" security rating. Regarding contract categories, the patient portal of medical centers and regional hospitals were evaluated as "low to medium risk" in most cases (62.5% for the former and 43.2% for the latter). Compared to medical centers and regional hospitals, most district hospital patient portals were evaluated as "high risk" security rating (47.4%). The association between security rating and contract category is identified (P<0.001, chi-square test). Regarding the hospital type, the patient portal of general hospitals were evaluated as "low to medium risk" security rating in most cases (42.7%). Compared to general hospitals, most ordinary and other hospital patient portals were evaluated as "high risk" security rating, with a proportion of 47.0% and 57.8%, respectively. The association between security and hospital type is also identified (P<0.001). However, no association was found between security and hospital location (P = 0.107).

Figure 5 lists the most common website weaknesses of patient portals reported by UPGARD. The first column shows the weakness type and the second column shows more detailed descriptions. The weakness "SSL not available" means the website does not support SSL protocol, which is the standard encryption method for browsing websites. If SSL is not available, the transferred data will be plain text, which easily leads to man-in-the-middle attacks. Another relative type of weakness called "HTTP still accessible", meaning the websites support SSL protocol but are not forced its users to use, so when users browse websites using pure HTTP protocol, the transferred data will still be plain text. To solve the above two weaknesses, the websites must support SSL protocol and force its users to use SSL protocol for communication. The "X-Powered-By header exposed" is one of information leakage weaknesses. The "X-Powered-By header", which responses detailed web server information, such as web server version, to web users. Black hat Hackers can collect important web server info exposed by "X-Powered-By header" and focus on the reported web server version to attack. The simplest way to solve "X-Powered-By header exposed" weakness is to disable "X-Powered-By header" usage. Finally, "Secure cookies not used" means the user cookies are permitted to be transferred using pure HTTP protocol. As mentioned, it may lead to increased risk of third parties intercepting information contained in these cookies. The safer way is to use secure attributes of cookies to refuse plain-text transmission. To protect privacy, the results of vulnerability scan of individual hospitals are not shown.

Table 1 Comparison Between Security Rating, Contracted Category, Hospital Type and Location

	Total (n=373)	Security rating				*P* value
		Absolute low risk (n=20)	Low to medium risk (n=104)	Medium to high risk (n=99)	High risk (n=150)	
	N	%	%	%	%	
Contracted category						<0.001
Medical centers	24	(0.0%)	(62.5%)	(29.2%)	(8.3%)	
Regional hospitals	81	(9.9%)	(43.2%)	(21.0%)	(25.9%)	
District hospitals	268	(4.5%)	(20.1%)	(28.0%)	(47.4%)	
Hospital type						<0.001
General hospitals	143	(6.3%)	(42.7%)	(25.2%)	(25.9%)	
Ordinary hospitals	185	(4.3%)	(18.9%)	(29.7%)	(47.0%)	
Other hospitals	45	(6.7%)	(17.8%)	(17.8%)	(57.8%)	
Hospital location						0.107
Municipality	233	(4.3%)	(25.3%)	(25.3%)	(45.1%)	
County	118	(7.6%)	(33.1%)	(30.5%)	(28.8%)	
City	22	(4.5%)	(27.3%)	(18.2%)	(50.0%)	

Weakness type	Description
SSL not available	SSL is the standard encryption method for browsing websites. If not available, the transferred data will be plain text
HTTP still accessible	The website is still accessible over HTTP. HTTP is an unsafe protocol for web site compared to HTTPS
X-Powered-By header exposed	The X-Powered-By header reveals information about specific technology used on the server
Secure cookies not used	When secure cookies are not used, there is an increased risk of third parties intercepting information contained in these cookies.

Figure 5 The common patient portal weaknesses of EEC member hospitals.

Discussion

First Finding

We found that a large proportion (40.2%) EEC member hospitals were evaluated as "high risk" security rating with UPGUARD, indicating that there is still room for hospitals to improve their patient portal security. This finding could be a warning for hospitals to improve their patient portal security. Recent research has also shown an alarming increase in cyberattacks to patient portals[33] and patient portal security should be enhanced. It is highly recommended that all medical institutes scan their websites and fix found weaknesses, especially for checking if the most common weaknesses listed in Figure 5 exist.

Second Finding

We found positive associations between contract category and hospital type with patient portal security of EEC member hospitals. Regarding contract categories, the patient portal of medical centers and regional hospitals were evaluated as "low to medium risk" security rating in most cases. Compared to medical center and regional hospital, most of the patient portals of district hospitals were evaluated as "high risk" security rating, which implies that medical centers and regional hospitals had better website security than district hospitals in general.

The contract category represents the hierarchy of medical care in Taiwan. The high-tier hospitals, such as medical centers and regional hospitals, generally had more resources to invest in patient portal security. Most of them even established their own departments of information security with expert personnel to prevent hacking. The low-tier hospitals, such as district hospitals and clinics, had no such security departments and had limited budget on security. It is likely the main reason why the patient portal security of district hospitals was worse than that of medical centers and regional hospitals. Similarly, general hospitals had better website security than ordinary hospitals and other hospitals. Compared to ordinary hospitals and other hospitals, general hospitals are of relatively larger scales, and they can afford to invest in website security, potentially leading to better patient portal security. Similar findings were observed in small and medium-sized enterprises that are deemed to be the least mature and highly vulnerable to cybersecurity risks due to budgetary constraints, and lack of cybersecurity expertise and personnel.[29,34,35]

In prior research, the interoperability and efficiency of EMRs exchange has been widely discussed.[7,36] However, the information security of EMRs exchange has not been adequately assessed. Under the EEC architecture, member hospitals shared their EMRs across institutes. That means hacking into any single member hospital could lead to EMRs leaking of other member hospitals. For example, successful black hat hackers can utilize compromised member

hospitals to request EMRs from other hospitals. Member hospitals, even a single one, with security weaknesses, can therefore pose security risks for the entire EEC. To make the situation worse, a majority of EEC member hospitals are district hospitals (268) and clinics (5872). In our study, we found that 47.4% of district hospital patient portals were evaluated as "high risk" security rating (Table 1), a proportion that is significantly higher than medical centers (8.3%) and regional hospitals (25.9%). This finding may be helpful for government or information security researchers to improve EEC safety. For example, enhancing patient portal security in low-tier hospitals is imperative. Possible solutions include government sponsorship of expenditure for patient portal security or regular risk assessments for patient portal security of EEC member hospitals.

Contribution

To the author's knowledge, our study is the first paper that indeed surveyed cybersecurity of patient portals with practical website security assessment methodology and found the common weaknesses of patient portals. Although we focus on patient portals in Taiwan, our proposed website security assessment methodology is suitable for assessing patient portal security in world-wide hospitals and helps identify weaknesses of patient portals. This paper also found that the association between patient portal security and hospital scale with statistical analysis. Large-scale hospitals generally had higher security levels, implying that the security of low-tier and small-scale hospitals needs to be reinforced. These findings could be utilized for better patient portal security and higher EMR privacy and confidentiality protection.

Limitations

Although the increasing risk of health information breaches may deter the adoption of EMR systems,[37] the recent SARS-Cov-2 pandemic provided impetus for the uptake of EMR systems. For example, during the time of SARS-Cov-2, the frequency of patient portal usage has increased dramatically,[38,39] which is the main motivation of our study to survey the patient portal security in 2022.

Our study focused on the patient portal security of hospitals but not on the internal physician systems used by healthcare professionals because physician systems are unreachable from the Internet and do not directly suffer cyberthreat. However, the security of physician systems is also worthy of attention. Although physician systems are unreachable from the Internet, they are often targeted as valuable hosts for lateral movement, which is a famous technique used by hackers to move through other systems in the same network after gaining initial access. For example, when hackers intrude into a patient portal, they gain initial access to HIS. By lateral movement,[40] hackers can exploit other internal security vulnerabilities within the enterprise network, such as insufficient protection of sensitive data and lack of access controls, to explore other internal systems of HIS, such as physician systems. Thus, the security of physician systems is worth surveying in future studies.

Conclusions

We found that the patient portal security of hospitals in Taiwan had association with hospital scale. Large-scale hospitals generally had higher security levels, implying that the security of low-tier and small-scale hospitals needs to be reinforced. The solution includes more government supervision of low-tier and small-scale hospitals. Especially for preservation of EHRs, critical regarding personal information privacy, needs a well-designed HIS for protection. Known weaknesses of patient portals need to be rectified. We recommend hospitals should pay attention to the risk assessment of their HIS, and should promptly fix weaknesses of their patient portal websites using vulnerability scanners, and should develop better cooperation to ensure the security of EMR exchange. The future work includes security risk assessment for internal physician systems of HIS.

Data Sharing Statement

The datasets used during the current study are available in https://www.nhi.gov.tw/Content_List.aspx?n=07FEBAA0B8C34D90&topn=D39E2B72B0BDFA15.

Disclosure

The authors report no conflicts of interest in this work.

References

1. Appar A, Johnson ME. Information security and privacy in healthcare: Current state of research.*Int. J Internet Enter Manag*. 2010;6:279–314. doi:10.1504/IJIEM.2010.035624
2. Samy GN, Ahmad R, Ismail Z. Security threats categories in healthcare information systems. *Health Informat J*. 2010;16:201–209. doi:10.1177/1460458210377468
3. Tapuria A, Porat T, Kalra D, Dsouza G, Xiaohui S, Curcin V. Impact of patient access to their electronic health record: systematic review. *Inform Health Soc Care*. 2021;46(2):192–204. doi:10.1080/17538157.2021.1879810
4. Petrovskaya O, Karpman A, Schilling J, et al. patient and health care provider perspectives on patient access to test results via web portals: Scoping review. *JMIR Med Inform*. 2022;10(7):7.
5. Antonio MG, Petrovskaya O, Lau F. The state of evidence in patient portals: Umbrella review. *J Med Internet Res*. 2020;22(11):e23851. doi:10.2196/23851
6. Lyles CR, Nelson EC, Frampton S, Dykes PC, Cemballi AG, Sarkar U. Using electronic health record portals to improve patient engagement: research priorities and best practices. *Ann Intern Med*. 2020;172(11 Suppl):S123–S129. doi:10.7326/M19-0876
7. Wen HC, Chang WP, Hsu MH, Ho CH, Chu CM. An Assessment of the Interoperability of Electronic Health Record Exchanges Among Hospitals and Clinics in Taiwan. *JMIR Med Inform*. 2019;7(1):e12630. doi:10.2196/12630
8. Gandhi VK. An Overview Study on Cyber crimes in Internet. *J Inform EngAppl*. 2012;2:1–5.
9. Parikh TP, Patel AR. Cyber security: study on Attack, Threat, Vulnerability. *Int J Res Mod Eng Emerg Tech*. 2017;5:1–7.
10. Bhatia P, Sehrawat R. Type of security threats and its prevention. *Int J Sci Res Dev*. 2012; 2.
11. Abomhara M, Kien GM. Cyber Security and the Internet of Things: vulnerabilities, Threats, Intruders and Attacks. *J Cyber Secur Mobil*. 2015;4:65–88. doi:10.13052/jcsm2245-1439.414
12. Conteh NY, Schmick PJ. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. *Int J Adv Comput Res*. 2016;6:31–38. doi:10.19101/IJACR.2016.623006
13. Choo KR. The cyber threat landscape: challenges and future research directions. *ComputSecur*. 2011;30:719–731.
14. Amarendra K, Mandhala VN, Damecharla S, Gollapudi P, Ponuganti PK. Modern Era Hacking. *Int J Sci Technol Res*. 2019;8:920.
15. Alsalim M, Alsalim A, Al-madhagi A, Shahen S. INFORMATION SECURITY THREATS: COMPUTER HACKING. *Int J Adv Res*. 2017;5:349–356. doi:10.21474/IJAR01/2753
16. Dashora K. Cyber Crime in the Society: problems and Preventions. *J Alter Perspect SociSci*. 2011;3:240–259.
17. Pavlik K. Cybercrime, Hacking, And Legislation. *J Cyber Res*. 2017;1:13–16.
18. Madarie R. Hackers' motivations: Testing Schwartz's theory of motivational types of values in a sample of hackers. *Int J Cyber Crim*. 2017;11:78–97.
19. Fan CM Security policy for hospitals and medical Industry influence. Available from https://s.itho.me/cybersec/2020/slides/8622.pdf. [accessed Nov 9, 2023].
20. Shah N, Farik M. Ransomware - Threats, vulnerabilities and recommendations. *Int J Sci Technol Res*. 2017;6:307–309.
21. Aurangzeb S, Aleem M, Iqbal MA, Islam MA. Ransomware: a Survey and Trends. *J Inf Assur Secur*. 2017;12:48–58.
22. Kansagra D, Kumhar M. Ransomware: a Threat to Cyber security. *Int J Comp Sci Communic*. 2016;7:224–227.
23. Idrissi SE, Berbiche N, Guerouate F, Sbihi M. Performance evaluation of web application security scanners for prevention and protection against vulnerabilities. *Int J ApplEng Res*. 2017;12:11068–11076.
24. Sheikh BA, Rajmohan P. Internet banking, security models and weakness. *Int J Res Manag Bus Stud*. 2015;2:17–22.
25. Bhatt D. Cyber security risks for modern web applications: Case study paper for developers and security testers. *Int J Sci Technol Res*. 2018;7:232–235.
26. Alabady S. Design and Implementation of a network security model for cooperative network. *Int Arab J e-Tech*. 2009;1:26–36.
27. Charoen D. Password Security. *Int J Secur*. 2014;8:1–14.
28. Gitanjali ST, Sasikala D. Vulnerability assessment of web applications using penetration testing. *Int J Recent Tech Eng*. 2019;8:1552–1556.
29. Sukumar A, Mahdiraji HA, Jafari-Sadeghi V. Cyber risk assessment in small and medium-sized enterprises: a multilevel decision-making approach for small e-tailors. *Risk Anal*. 2023;43(10):2082–2098. doi:10.1111/risa.14092
30. NIST. The NIST Cybersecurity Framework (CSF) 2.0. Available from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf. Accessed May 11, 2024.
31. Patil HP, Gosavi PB. web vulnerability scanner by using HTTP method. *Int J Comput Sci Mobile Comput*. 2015;4:255–260.
32. Mike B. Free Website Security Scan. Available fromhttps://webscan.upguard.com/. Accessed May 11, 2024.
33. Hosseini N, Fakhar F, Kiani B, Eslami S. Enhancing the security of patients' portals and websites by detecting malicious web crawlers using machine learning techniques. *Int J Med Inform*. 2019;132:103976. doi:10.1016/j.ijmedinf.2019.103976
34. Manzoor J, Waleed A, Jamali AF, Masood A, Kovtun V. Cybersecurity on a budget: evaluating security and performance of open-source SIEM solutions for SMEs. *PLoS One*. 2024;19(3):e0301183. doi:10.1371/journal.pone.0301183
35. Ilca LF, Lucian OP, Balan TC. Enhancing cyber-resilience for small and medium-sized organizations with prescriptive malware analysis, Detection and response. *Sensors*. 2023;23(15):6757. doi:10.3390/s23156757
36. Li YC, Yen JC, Chiu WT, Jian WS, Syed-Abdul S, Hsu MH. Building a national electronic medical record exchange system - experiences in Taiwan. *Comput Meth Progr Biomed*. 2015;121(1):14–20. doi:10.1016/j.cmpb.2015.04.013
37. Seh AH, Zarour M, Alenezi M, et al. Healthcare Data Breaches: insights and Implications. *Healthcare*. 2020;8(2):133. doi:10.3390/healthcare8020133
38. Stanimirovic D. eHealth Patient Portal - Becoming an Indispensable Public Health Tool in the Time of Covid-19. *Stud Health Technol Inform*. 2021;281:880–884. doi:10.3233/SHTI210305
39. Portz JD, Brungardt A, Shanbhag P, et al. Advance Care Planning Among Users of a Patient Portal During the COVID-19 Pandemic: retrospective Observational Study. *J Med Internet Res*. 2020;22(8):e21385. doi:10.2196/21385
40. Shi Y, Chang X, Rodríguez RJ, Zhang Z, Trivedi KS. Quantitative security analysis of a dynamic network system under lateral movement-based attacks. *Reliab Eng Syst Saf*. 2019;183:213–225. doi:10.1016/j.ress.2018.11.022