Free Web-based Personal Health Records: An Assessment of Security and Privacy

Inma Carrión, José-Luis Fernández-Alemán and Ambrosio Toval

Department of Informatics and System, Faculty of Computer Science, University of Murcia, Murcia, Spain

Abstract. Several obstacles prevent the adoption and use of Personal Health Record (PHR) systems, including users' concerns regarding the privacy and security of their personal health information. The purpose of this study is to examine current PHR systems in order to verify what privacy and security characteristics are deployed in them, in an American context. The strengths and weaknesses of the PHRs identified will be useful for PHR users, healthcare professionals, decision makers and builders. The myPHR website was reviewed since it contains relevant information related to PHRs. For this end, the Privacy Policy of each PHR selected was reviewed in order to extract the main characteristics of privacy and security. The results show that the Privacy Policies of PHR systems do not provide an in-depth description of the security measures that they use. This may be a problem because users might not believe that their data are really protected. The designs of Privacy Policies should be improved to include more detailed information related to security measures, and this may be one of the reasons why users do not trust in PHR systems.

1 Introduction

A PHR is "an electronic record of an individual's health information by which the individual controls the access to the information and may have the ability to manage, track, and participate in his or her own health care" [1]. Nevertheless, several important obstacles prevent the adoption and use of PHR systems, including concerns regarding the privacy and security of users' data [2]. Most PHR development and current use is in the US, what justifies a certain US focus in this paper. Ninety-one percent of American people state that they are very worried about the privacy and security of their health information [3]. Moreover, the consequences of an attack include reductions in the quality of care, service disruptions, reduced revenues, higher operating costs, regulatory fines, unsecured privacy and unauthorized access to personal information [4]. Our objective is to analyze the main characteristics related to security and privacy in PHR systems to verify what security measures are deployed. The strengths and weaknesses in matters of the privacy and security of PHRs will be useful for PHR users, healthcare professionals, decision makers and builders.

The aim of this review is to answer the following research question (RQ):

RQ1 What security and privacy features do current PHR systems have?

Carrión I., Fernández-Alemán J. and Toval A..
Free Web-based Personal Health Records: An Assessment of Security and Privacy.
DOI: 10.5220/0004090800610068
In *Proceedings of the 9th International Workshop on Security in Information Systems* (WOSIS-2012), pages 61-68
ISBN: 978-989-8565-15-0

In this paper, the privacy policies of 24 free web-based PHRs are analyzed and assessed. The authors have verified that the information contained in the Privacy Policies is met by PHRs. The remainder of the paper is organized as follows. Section 2 introduces the research method. Section 3 offers the main results of the data collected. The main findings are discussed in Section 4. Finally, Section 5 presents some concluding remarks.

2 Methods

2.1 Review, Protocol and Eligibility Criteria

This review followed the quality reporting guidelines set out by the Preferred Reporting Items for Systematic reviews and Meta-Analysis (PRISMA) group [5]. We developed a review protocol describing each step of the process (including eligibility criteria), even before beginning the search for literature and data extraction. This protocol was performed by one of the authors, and was reviewed and approved by the other two.

The following inclusion criteria were used:

IC1 Free PHRs
IC2 PHRs with a Web-based format
IC3 PHRs with a Privacy Policy

Among the current variety of PHR support technologies, we have focused our study on Web-based, free PHRs. Free PHRs can be used by anyone and are easier to access (IC1). Web-based PHRs have certain benefits with regard to the use of the Internet (IC2). Finally, we defined IC3 because our study is based on the analysis of Privacy Policies. Privacy Policy is a document that involves the manners in which the client information is used, disclosed and managed by the company/provider.

2.2 Information Sources and Study Selection

The majority of the PHRs were published on the myPHR website. This website was created by the American Health Information Management Association (AHIMA) and contains information related to the use and the creation of PHRs. To the best of our knowledge, this website provides the most comprehensive list of PHRs that a user can find, and has also been used to select PHRs in multi-source sampling [6].

The PHR selection was organized in the following four phases:

1) The search for PHRs from the myPHR website; 2) The exploration of the PHRs found, and a selection based on eligibility criteria IC1 and IC2; 3) The exploration of the PHR websites identified in order to find each one's Privacy Policy (IC3); 4)A complete reading of each of the PHR Privacy Policies selected in the previous phase to extract their principal privacy and security characteristics.

2.3 Data Collection Process and Data Items

Data collection was carried out by using a data extraction form. Each PHR was assessed by two of the authors of the work presented herein who read the full texts of the Privacy Policies, and any discrepancies were resolved by the third author. These PHR Privacy Policies were used to extract the methods used to maintain the privacy and security of the users' data. The privacy policy should satisfy the security safeguards that are appropriate to the sensitivity of the information, and will be used for protecting personal information [7].

This study analyzes security based on ISO 13606 standard [8]. Security is analyzed from the standpoint of availability, confidentiality, integrity and accountability. ISO 13606 standards do not included privacy characteristics, and this topic was analyzed according to Westin, who defined the privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" [9].

A template was designed which contained the data that should be extracted from each PHR. In total, 23 characteristics were analyzed and grouped into five categories. Each of them satisfied one or more of the eight principles concerning Privacy Policies by the Canadian Standards Association [7].

Account Management (AM) describes the data management when the users' accounts are deleted, along with the account types defined in the PHR system.

1. Deleted by the user (AM1). The PHR mentions in its Privacy Policy how it manages the users' data when the individuals remove their accounts.
2. Account types (AM2).

Access Management (ASM). describes who shares the information, with whom it is shared, and types of permissions.

1. Users grant access (ASM1).
2. Users grant healthcare professionals access (ASM2).
3. Users grant others roles access (ASM3) (like friends, family, or applications).
4. Permission types (ASM4).
5. Access in case of emergency (ASM5).

Access criteria (AC). The system must establish what actions the user is permitted to perform on that resource.

1. Roles (AC1). The role is based on a job assignment or function.
2. Time (AC2). Access is only permitted for a period of time.

Authentication (AU). Method used to prove that the user is who s/he says s/he is.

1. Something known (AU1) (like a password, PIN, etc.).
2. Something had (AU2) (a key, an access card, a badge, etc.).

Safeguards (S). This category describes security measures deployed by the PHR system.

1. Physical security measures (S1).

2. Access limited (S2). Computer servers with access limited to a small number of people.
3. Electronic security measures (S3).
4. Encrypted data (S4).
5. Back-up system (S5).
6. Data security plan defined (S6).
7. Staff training (S7). The staff receives training on the latest security technology.
8. Privacy Seal (S8). The PHR website has obtained certification from, for example, TRUSTe. This certification indicates that the site has been self-certified as complying with the site's own privacy statement.

2.4 Quality Assessment

Each PHR was evaluated depending on the characteristics which were satisfied in it. Three different scores were assigned to each PHR: Total Score, Security Score and Privacy Score. The Total Score was obtained by adding one point to the PHR for each characteristic that was satisfied. The privacy and security scores group the characteristic categories related to information privacy and security, respectively. The categories were grouped as follows, in accordance with the security and privacy definitions described in Section 2.3:

Total All categories defined in Section 2.3
Security Access Criteria, Authentication, Safeguards
Privacy Access Management

The privacy policies were assessed by two researchers with experience in this field, and were then cross-checked against an evaluation of 50% of the PHRs. The Cohen's Kappa coefficient was used to calculate the interrater agreement among the two researchers in the privacy policy evaluation. The Kappa coefficient was 0.95, which, according to Landis and Koch [10], indicates an almost perfect agreement between the two assessments.

3 Results

A total of 24 PHRs were identified in the review. The search of the myPHR website provided a total of 52 different PHRs, although 11 were discarded because they did not satisfy the IC1 criterion. Another 13 PHRs were then discarded because they clearly did not satisfy the IC2 criterion. The Privacy Policies of the remaining 28 PHRs were examined, and 4 of these were discarded because they did not find their Privacy Policies (IC3). Table 1 shows the results obtained after analyzing each PHR, indicating the characteristics which are satisfied by each one.

4 Discussion

With regard to PHR access management, sixteen PHRs allow users to grant and revoke access to their data. This characteristic is particularly important because users require

Table 1. Description of PHRs, indicating characteristics satisfied.

PHR	AM	ASM	AC	AU	S
dLife				AU1	S1, S8
Dr. I-Net		ASM1, ASM2		AU1	S1, S3, S4
EMRy STICK		ASM1		AU1	
Google Health	AM1	ASM1, ASM2, ASM3, ASM4		AU1	S1, S2, S3, S4, S5
HealthButler	AM1, AM2	ASM1, ASM2	AC1	AU1	
Healthy Circles	AM1, AM2	ASM1, ASM2, ASM4	AC1	AU1	S1, S3, S8
iHealthRecord			AC1	AU1	S1
Juniper Health		ASM1		AU1	S1, S2, S3, S4, S8
Keas				AU1	S1, S3
MedicAlert		ASM1, ASM5	AC1	AU1	S1, S3, S5, S7
MediCompass		ASM1, ASM2	AC1	AU1	S1, S3, S4
MedsFile.com			AC1	AU2	S1, S2
Microsoft HealthVault	AM1	ASM1, ASM3, ASM4, ASM5	AC2	AU1	S1, S2, S3, S4, S8
MyChart			AC1	AU1	
My Doclopedia		ASM1, ASM2		AU1	S3
My HealtheVet			AC1	AU1	S3, S4
myHealthFolders	AM1	ASM1, ASM2, ASM5	AC1	AU1	S1, S3, S4
myMediConnect		ASM1, ASM2, ASM5		AU1	S1, S3, S4
NoMoreClipBoard		ASM1, ASM2, ASM5	AC1	AU1	S3, S4
MediCompass		ASM1, ASM2	AC1	AU1	S1, S3, S4
PatiensLikeMe		ASM1, ASM4, ASM5		AU1	
RememberItNow!		ASM1, ASM2, ASM3, ASM4	AC2	AU1	S2, S3, S4
Telemedical		ASM1	AC1	AU1	S3, S4, S5
VIA		ASM1	AC1, AC2	AU1	S1, S3, S4
ZebraHealth			AC1	AU1	S1, S3, S5, S6

more flexible ways in which to share data and links with health professionals [11]. EnCoRe [12], a research project performed by the UK industry and members of academia, investigates how to make an individual's consent a useful means to control what happens to the personal information they disclose to organizations. These issues are related to PHR access management

One characteristic not found in the PHRs reviewed is that of notifying users when their data have been exposed. Users have the right to know this, but the designers have not taken this issue into account because the inadvertent disclosure or loss of unencrypted Protected Health Information (PHI) would be considered as a data breach. Most states in the US have data breach notification laws [13]. These require a data custodian to report a data breach to the individuals affected, state attorneys general, the media, consumer reporting agencies, and/or other government agencies. One means to ensure that users trust their data's security is to obtain a certification for the PHR website from a certificate authority.

The PHR systems should take measures to protect user information. These measures should be physical and electronic for total protection. The physical security measures attempt to protect the servers which contain the users' data. The principal electronic security measures involve the encryption of any users' data that is stored in and transmitted over the network. The process of encryption hides data or the contents of a message in such a way that the original information can be recovered through a corresponding decryption process to ensure that message data are not disclosed. Some PHRs (17%)

explicitly indicate in their Privacy Policy that the data are encrypted both for transmission and storage. However, encryption is only part of the solution which keeps the data protected. There are also other threats, such as a virus laden-system, against which the PHR systems must be protected.

The security measures deployed by PHRs are an important question, particularly for the PHRs included in this review which are Web-based, thus increasing the vulnerability of these applications, systems, and sensitive data. An attacker who successfully exploits application vulnerability could quickly and significantly affect a healthcare facility in a variety of ways, such as disrupting services, stealing data and identities, or taking control of host computers and using them for illicit purposes [14]. Since there are no well documented examples of PHR/EHR (Electronic Health Record) systems linked to security breaches [15], designers should consider threats to Web applications at least when they deploy their PHR. In 2008, over 63% of all documented vulnerabilities concerned Web applications [16]. Moreover, the National Institute of Standards and Technology (NIST) has identified 46467 Common Vulnerabilities and Exposures (CVE) between 1997 and 2011, which have been grouped into categories. Of these, Cross-Site Scripting (XSS), the most important categories of vulnerabilities that affect Web applications, has 2823 CVEs [17]. This is just one example of the amount of threats which could affect Web-based PHRs and should be carefully considered in their design.

Finally, all the PHRs analyzed used only one authentication method, using something which the users know or have. However, two of the following three methods are recommended for inclusion in an identification system: “something a person knows” such as login ID, email address, password, PIN; “something a person has” such as a key, swipe card, access card, digital certificate; or “something that identifies a person” such as biometrics. Designers should incorporate another authentication system in order to provide strong authentication [18]. Moreover, the use of passwords as authentication mechanisms is exposed to multiple types of attacks, such as “electronic monitoring” for listening to network traffic to capture information, or ”unauthorized access the password file“.

4.1 Final Evaluation

Few differences have been found, and those that have appeared have occurred because the PHR has a particular functionality which is not described in the Privacy Policy. This error is not grave: users are simply not informed about those functionalities. If a particular functionality were not deployed, but was stated in the Privacy Policy, the designers would be making a serious error, since the users are being deceived. The scores calculated in Section 3 help us to compare the PHRs. Figure 1 shows a histogram of the privacy and security scores obtained by the PHRs. In general, the PHRs obtain a privacy score that is higher than the security measure score deployed. PHR designers should therefore focus their efforts on increasing the quality of security measures at all stages of the PHR development [19].

5 Conclusions

In accordance with the Privacy Policies, PHRs do not provide an in-depth description

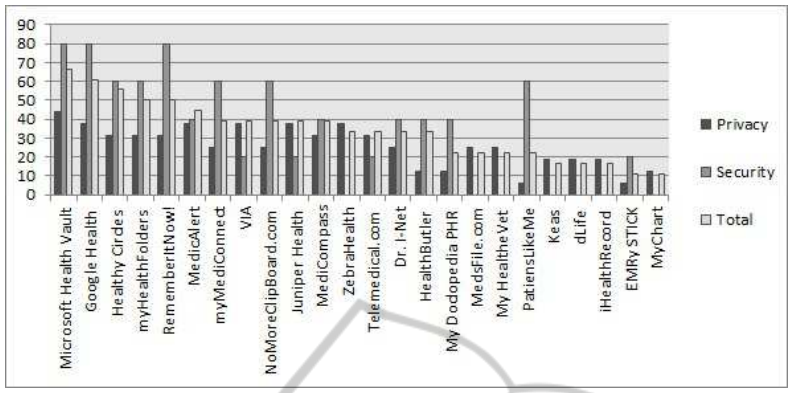

Fig. 1. Histogram of the Privacy and Security Scores of PHRs.

of the security measures used, which might be a problem, leading users to be concerned about whether their data are really protected. The designs of Privacy Policies also need to be improved to include more detailed information related to security measures. These findings can be extended to any web system.

Our study may have some limitations, such as the following: (1) the authors may have not included PHRs relevant for this study; (2) the authors may have not included PHRs in which a Privacy Policy is defined, when this was not mentioned on the PHR's website; (3) lack of analysis of user's perceptions or actions with regard to this topic; (4) lack of analysis of important privacy issues.

The development of third party applications that add new functionality to PHRs is increasing. An example of this is Microsoft HealthVault which has more than 50 third party applications at the present. This connection to other applications, such as PHRs, could cause security breaches. Moreover, some PHRs use cloud computing, such as Microsoft which provides a PHR which offers cloud-computing services through its API. Some PHRs, like HealthATM, have been deployed around Microsoft HealthVault, thus making it possible to design low-cost PHRs that are customized for specific functions and populations. However, PHRs which offer cloud services must consider the new arising security and privacy threats [20]. The goals are involved in achieving adequate security: availability, confidentiality, data integrity, control and auditing [21].

Future research involves to perform a deep analysis about threats related to PHRs, detailing them and the actors, the expected impact and likelihood, and corresponding requirements and countermeasures.

Acknowledgements

This work has been partially financed by the Spanish Ministry of Science and Innovation, project PANGEA, TIN2009-13718-C02-02

References

1. HHS - OCR: Personal Health Records and the HIPAA Privacy Rule (2008)

2. Liu, L.S., Shih, P. C., Hayes, G. R.: Barriers to the adoption and use of personal health record systems. In: Proceedings of the 2011 iConference. iConference '11, New York, NY, USA, ACM (2011) 363–370
3. Kaelber, D. C., Jha, A. K., Johnston, D., Middleton, B., Bates, D. W.: A research agenda for personal health records (phrs). J Am Med Inform Assoc 15 (2008) 729–736
4. Mellado, D., Fernández-Medina, E., Piattini, M.: Security requirements engineering framework for software product lines. Information & Software Technology 52 (2010) 1094–1117
5. Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., G¸tzsche, P. C., Ioannidis, J. P., Clarke, M., Devereaux, P., Kleijnen, J., Moher, D.: The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration. Journal of Clinical Epidemiology 62 (2009) e1–e34
6. Hulse, N. C., Wood, G. M., Haug, P.J., Williams, M. S.: Deriving consumer-facing disease concepts for family health histories using multi-source sampling. J Biomed Inform 43 (2010) 716–724
7. Yee, G., Korba, L.: Personal Privacy Policies. Computer and Information Security Handbook. (2009)
8. ISO: Norma ISO/CEN 13606. Available from: www.aenor.es (2010)
9. Westin, A.: Privacy and Freedom. Atheneum, Ed. NY (1967)
10. Landis, J. R., Koch, G. G.: The measurement of observer agreement for categorical data. Biometrics 33 (1977) 159–174
11. Greenhalgh, T., Hinder, S., Stramer, K., Bratan, T., Russell, J.: Adoption, non-adoption, and abandonment of a personal electronic health record: case study of healthspace. BMJ 341 (2010) c5814
12. UK industria & academia: EnCoRe. Ensuring Consent and Revocation. http://www.encore-project.info/index.html (2010)
13. Lesemann, D.: Once more unto the breach: An analysis of legal, technological and policy issues involving data breach notification statutes. Akron Intellectual Property Journal 4 (2010) 203
14. Brigade, T.: The new threat: Attackers that target healthcare (and what you can do about it). Technical report, http://www.infosecwriters.com/text_resources/pdf/New_Threat_Brigade.pdf (2006)
15. Greenhalgh, T., Stramer, K., Bratan, T., Byrne, E., Russell, J., Hinder, S., Potts, H.: The devil's in the detail: Final report of the independent evaluation of the summary care record and healthspace programmes. Technical report, University College London (2010)
16. Huynh, T., Miller, J.: An empirical investigation into open source web applications' implementation vulnerabilities. Empirical Software Engineering 15 (2010) 556–576
17. NIST Vulnerabilities Database: CWE - Common Weakness Enumeration. http://nvd.nist.gov/cwe.cfm. archived at: http://www.webcitation.org/60iaz4jzw (2011)
18. Park, M. A.: Embedding security into visual programming courses. In: Proceedings of the 2011 Information Security Curriculum Development Conference. InfoSecCD '11, New York, NY, USA, ACM (2011) 84–93
19. Fernandez-Medina, E., Piattini, M.: Designing secure databases. Information & Software Technology 47 (2005) 463–477
20. Carrión, I., Fernández Alemán, J. L., Toval, A.: Personal Health Records: New Means to Safely Handle our Health Data? Computer (2012)
21. Rebollo, O., Mellado, D., Fernández-Medina, E.: A Comparative Review of Cloud Security Proposals. In: WOSIS. (2011) 3–12