


RESEARCH

Open Access



# Integrated personal health record (PHR) security: requirements and mechanisms

Azamossadat Hosseini<sup>1</sup>, Hassan Emami<sup>2</sup>, Yousef Sadat<sup>3</sup> and Somayeh Paydar<sup>4\*</sup> 

## Abstract

**Background** Personal Health Records (PHRs) are designed to fulfill the goals of electronic health (eHealth) and empower the individual in the process of self-care. Integrated PHR can improve the quality of care, strengthen the patient-healthcare provider relationship, and reduce healthcare costs. Still, the process of PHR acceptance and use has been slow and mainly hindered by people's concerns about the security of their personal health information. Thus, the present study aimed to identify the Integrated PHR security requirements and mechanisms.

**Methods** In this applied study, PHR security requirements were identified with a literature review of (library sources, research articles, scientific documents, and reliable websites). The identified requirements were classified, and a questionnaire was developed accordingly. Thirty experts completed the questionnaire in a two-round Delphi technique, and the data were analyzed by descriptive statistics.

**Results** The PHR security requirements were identified and classified into seven dimensions confidentiality, availability, integrity, authentication, authorization, non-repudiation, and right of access, each dimension having certain mechanisms. On average, the experts reached an agreement about the mechanisms of confidentiality (94.67%), availability (96.67%), integrity (93.33%), authentication (100%), authorization (97.78%), non-repudiation (100%), and right of access (90%).

**Conclusion** Integrated PHR security is a requirement for its acceptance and use. To design a useful and reliable integrated PHR, system designers, health policymakers, and healthcare organizations must identify and apply security requirements to guarantee the privacy and confidentiality of data.

**Keywords** Security, Personal health record, Integrated PHR, personal health record security

## Background

The Personal Health Record (PHR) is an electronic, life-long resource of a person's health information to make health decisions. Individuals own, organize and manage the information in the PHR, which adds by both the individual and their healthcare provider. This health information is shared in a private, secure, and confidential environment with the individual determining rights of access by the PHR owner [1, 2]. PHRs are robust health information technology tools that regard patients as active factors in the healthcare decision-making process [3, 4].

\*Correspondence:

Somayeh Paydar  
somayeh.paydar@kums.ac.ir

<sup>1</sup>Health Information Management (HIM), Department of Health Information Technology and Management, School of Allied Medical Sciences, Shahid Beheshti University of Medical Sciences, Tehran, Iran

<sup>2</sup>Management of Technology, Department of Health Information Technology and Management, School of Allied Medical Sciences, Shahid Beheshti University of Medical Sciences, Tehran, Iran

<sup>3</sup>Health Information Management (HIM), Department of Health Information Technology, Faculty of Paramedicine, Hormozgan University of Medical Sciences, Bandar Abbas, Iran

<sup>4</sup>Health Information Management (HIM), Department of Health Information Technology, School of Paramedical Sciences, Kermanshah University of Medical Sciences, Kermanshah, Iran



© The Author(s) 2023. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>. The Creative Commons Public Domain Dedication waiver (<http://creativecommons.org/publicdomain/zero/1.0/>) applies to the data made available in this article, unless otherwise stated in a credit line to the data.

While there exists a variety of PHRs, there are three main categories of PHRs, which are as follows: (1) stand-alone or free-standing PHRs, which do not directly connect with any other systems and require manual data entry to populate and update the record. The most common types of these PHRs are either paper-based or personal computer-based; (2) tethered or institution-specific PHRs, which connect with the provider's electronic medical record (EMR), with the web-based network and insurance company; (3) integrated or interconnected PHRs can be connected to multiple data networks and institutions [5–7]. The ideal type is an integrated PHR that can empower patients to manage their health care and facilitate continuous communication between patients and their health providers [8]. This type of PHRs can connect, exchange, and share information with a variety of information resources such as electronic health records (EHRs), insurance companies, pharmacies, and patients themselves [3, 9]. The PHR complements and is considered to be an element of the EHR and it is more comprehensive than the EHR as it includes information added by individuals such as diet and exercise routine [10]. The data in PHR is under the ownership and control of the patient, but in EHR it is under the ownership of healthcare providers [11]. By using safe and standard tools, patients and their families can integrate and manage healthcare information; as such, integrated PHRs are valuable assets for these groups [12]. Patients' use of integrated PHR increases their awareness about healthcare, provides easier access to healthcare services, allows them to ask physicians questions, and helps them improve their health [13]. This electronic record empowers patients to self-manage their health, improves patient outcomes, decreases the cost of healthcare, enhances access to healthcare, especially in distance areas, and improves medication adherence [14]. Despite extensive efforts to increase patients' access to their medical information through PHR in recent years, several legal, ethical, and technical challenges have seriously hindered PHR implementation [8, 15]. To promote PHR acceptance and ensure its successful implementation, it is thus essential to identify and elucidate factors that affect patients' use of PHR [16]. Personal health information security is a major barrier to integrated PHR acceptance and usage [17–19]. The previous studies have discussed serious issues in implementing or using integrated PHR that is one of which was concern about the security of information [8, 20, 21].

Integrated PHR contains personal and health information that is sensitive information. Some people have concerns about storing and protecting this information online and consent to use them [8, 22]. Users' trust in healthcare providers greatly depends on their awareness and perception of PHR privacy and security [23].

To ensure this trust, comprehensive security and privacy framework are needed to provide transparent regulations for access to, use, and disclosure of personal health information in PHR [24]. Perceived security and privacy have a positive influence on users' attitudes and behavioral intentions in using integrated PHR to manage health information [25]. The establishment of private restrictions and security for information causes individuals to be able to control their personal information and guarantee its security and confidentiality [26].

According to the Markle Foundation's Personal Health Technology Council, ensuring the security of information, respecting users' privacy, and controlling their health records are essential to user acceptance of electronic information exchange and sharing integrated PHR [27]. Dimensions of data security and protection, including confidentiality, integrity, authentication, and availability should be included in PHR design and development for any activity that requires information storage and exchange [8, 26, 28]. As the breach of confidentiality and security of information poses an ethical barrier to the use of PHR, [28] the present study aimed to identify the requirements and mechanisms of integrated PHR security to guide PHR designers. In this article, we identified security requirements based on a literature review and categorized them into 7 dimensions that each dimension has different mechanisms. These requirements were confirmed by 30 experts in two rounds of the Delphi technique. For designing and implementing a reliable PHR, all identified security requirements and mechanisms should be considered.

## Methods

This applied study was developed via a two-stage process. In the first phase; to identify integrated PHR security requirements; a literature review was conducted by searching Web of Science, Scopus, PubMed, and Embase databases and websites of the American Health Information Management Association (AHIMA), the International Organization for Standardization (ISO), Health Level 7 (HL7). Then, security requirements were extracted from websites, online forms, and articles, and 7-dimensions of these requirements were selected based on the results of the literature review and research team view. A researcher-made questionnaire was designed based on the extracted requirements. The content validity of the questionnaire was confirmed by ten health information management and medical informatics experts.

In the second phase, the research team selects a group of experts based on the study topic as panel members of the Delphi technique. The selection of these experts was done by purposive random sampling method. Experts were Faculty members of health information management (10 experts) and medical informatics (10 experts)

of Medical Sciences Universities with at least 5 years of experience as academic staff and experts or officials of the Statistics and Technology Information Management Center (10 experts) of the Ministry of Health and Medical Education with 5 years of experience in the field of electronic health records and information technology projects. Then, two rounds of questionnaires are presented to experts, and responses are aggregated after each round. Collected responses after each round were analyzed via descriptive statistics (number and frequency percentage) in Microsoft Excel 2019. All the questions with a score of >75% achieved expert consensus, all the questions with a score of 50–75% entered the second Delphi round, and the questions with a score of <50% were eliminated in the first Delphi round. As such, another questionnaire was designed for the second Delphi round to apply the comments and modifications of the first round (Fig. 1).

**Results**

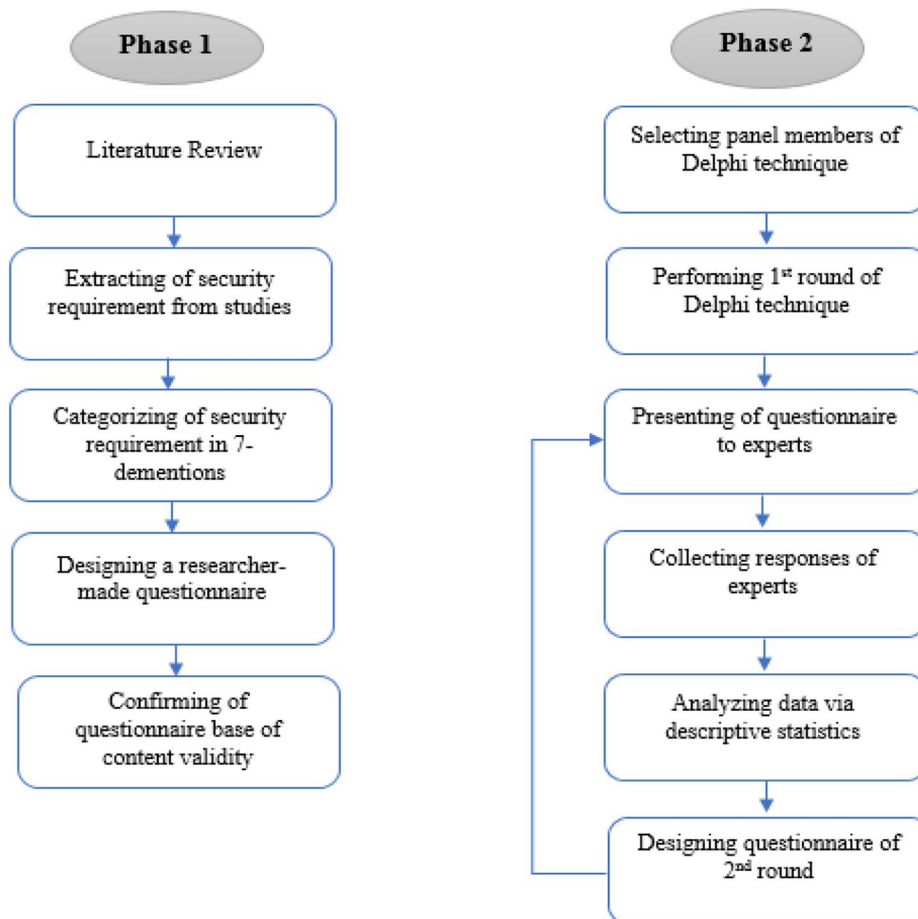
Seven dimensions were determined based on the first phase finding of the study that were obtained through the literature review. These seven dimensions were classified

into confidentiality, availability, integrity, authentication, authorization, non-repudiation, and access rights. Each dimension comprised certain mechanisms as shown in Table 1.

The findings of the first Delphi round indicate that the suggestions about PHR security requirements achieved an expert agreement of >76% (Table 2).

Among confidentiality requirements, “Restrictions of information updating by users unauthorized” received the lowest score with 6 “disagree”. Availability and authorization requirements (>93.33%) and integrity requirements (>86.67%) also achieved expert agreement. The experts also confirmed all the authentication and non-repudiation requirements (100%). Among the right of access requirements, “Revocation of entities’ access by PHR owner at any time” had the lowest score with 7 “disagree”, while the rest of the items attained >86% agreement.

The experts suggested “using reCAPTCHA to prevent bots from logging into the system” (authentication dimension) in the first Delphi round, and this item attained 100% agreement in the second Delphi round.



**Fig. 1** Diagram of the research method phases

**Table 1** Security Requirements and Mechanisms of integrated PHR

Requirements	Mechanisms
<b>Confidentiality</b>	<ul style="list-style-type: none"> <li>• Registering authorized PHR users</li> <li>• Determining the information sensitivity level in PHR</li> <li>• Encrypting data or key fields in PHR databases</li> <li>• Hiding information from unauthorized users</li> <li>• Restrictions of information updating by unauthorized users</li> </ul>
<b>Availability</b>	<ul style="list-style-type: none"> <li>• Creating an information backup</li> <li>• Specifying data access control list</li> </ul>
<b>Integrity</b>	<ul style="list-style-type: none"> <li>• Using a digital signature</li> <li>• Determining the standard terminology</li> </ul>
<b>Authentication</b>	<ul style="list-style-type: none"> <li>• Assigning user ID to all users</li> <li>• Determining password mechanisms</li> <li>• Using biometric scans (fingerprints, face, hands, retina)</li> </ul>
<b>Authorization</b>	<ul style="list-style-type: none"> <li>• Defining the roles (patient, provider, system manager, etc.)</li> <li>• Defining users' access level to information</li> <li>• Compiling user's list to access information in emergencies</li> </ul>
<b>Non-repudiation</b>	<ul style="list-style-type: none"> <li>• Creating an audit log (information audit)</li> <li>• Creating users' accountability for any changes and manipulations</li> </ul>
<b>Access right</b>	<ul style="list-style-type: none"> <li>• Determining the time and individual (authorized users) to access personal health data by PHR owner</li> <li>• Authorizing another user to access &amp; control the information for sharing by PHR owner</li> <li>• Reviewing entities' access to personal health data by PHR owner</li> <li>• Revocation of entities' access by PHR owner at any time</li> <li>• Restricting the previous physician's access right to PHR</li> </ul>

**Table 2** 1st Round of Security Requirements and Mechanisms of Integrated PHR

Security requirements & mechanisms		Experts Opinions			
		Agree		Disagree	
		Number	Percent	Number	Percent
Confidentiality	Registering authorized PHR users	28	93.33	2	6.67
	Determining the information sensitivity level in PHR	30	100	0	0
	Encrypting data or key fields in PHR databases	30	100	0	0
	Hiding Information from unauthorized users	30	100	0	0
	Restrictions of information updating by unauthorized users	24	80	6	20
Availability	Creating an information backup	28	93.33	2	6.67
	Specifying data access control list	30	100	0	0
Integrity	Using digital signature	26	86.67	4	13.33
	Determining the Standard terminology	30	100	0	0
Authentication	Assigning username to all user	30	100	0	0
	Determining Password mechanisms	30	100	0	0
	Using biometric scans (fingerprints, face, hands, retina)	30	100	0	0
Authorization	Defining the roles (patient, provider, system manager, etc.)	30	100	0	0
	Defining users' access level to information	28	93.33	2	6.67
	Compiling user's list to access information in emergencies	30	100	0	0
Non-Repudiation	Creating an audit log (information audit)	30	100	0	0
	Creating accountability of users for any changes and manipulations	30	100	0	0
Access Right	Determining the time and individual (authorized users) to access personal health data by PHR owner	28	93.33	2	6.67
	Authorizing another user to access & control the information for sharing by the PHR owner	28	93.33	2	6.67
	Reviewing entities' access to personal health data by PHR owner	30	100	0	0
	Revocation of entities' access by PHR owner at any time	23	76.67	7	23.33
	Restricting the previous physician's access right to PHR	26	86.67	4	13.33

## Discussion

This study discusses the security requirements of integrated PHR. Nowadays, a bidirectional flow between PHR and EHR systems is increasing for health care information exchange. Integrated PHRs combine EHR information from institutional medical records with patient self-reported data [29, 30]. A common concern for Designing of integrated PHR is information security and patient privacy [31, 32]. According to Harahap et al. study, the information security of integrated PHRs is ensured by mechanisms such as a single sign-on mechanism, authorization, user authentication, encryption or pseudonymization, backup mechanism, identity verification, and firewalls [8]. In our study, the dimensions of confidentiality, integrity, availability, authentication, authorization, non-repudiation, and right of access were identified as PHR security requirements. Mathuria et al. [33] and Israelson et al. [34] reported the security and right of access requirements to include patient information confidentiality, data integrity, authentication, authorization, non-repudiation, right of secure access to information, and access to information in emergencies. These findings are consistent with the current study.

Confidentiality as one of the security requirements assures that only authorized users can access PHR information and, as such, is a fundamental security requirement for sensitive PHR data. No unauthorized user should access PHR information unless authorized by the PHR owner [35]. The study results of Padol et al. indicated that patients are worried about unauthorized access, hacking, and lack of trust regarding their personal health information. They proposed solutions including HIPAA regulation, encryption and decryption, time stamp and control access [36]. The HIPAA regulations mandate that patients should have the right to access and receive a copy of their PHR. In addition, all healthcare systems (EHR, PHR, etc.) must adhere to HIPAA regulations, including the security, privacy, transfer, and release of patients' medical information; and patients should be able to consent to and authorize the sharing of their PHR data with EHR systems [31]. Also, other studies provide results in line with this study that confidentiality requirements and data integrity are earned through data encryption, hiding and anonymization [34, 37–40], registering authorized users (healthcare providers or other patient-designated users) [41], determining confidential information and the information sensitivity level in the PHR [42].

An essential feature of integrated PHR is adding the ability to import and export full or partial backups [43]. According to Harahap et al. [8], Coatrieux et al. [44], and Zhou et al. [45], a backup option as an availability mechanism can avoid data loss and provide audit logs to review what data have been accessed and who accessed them.

Integrity ensures that unauthorized users cannot manipulate PHR data [35]. According to the HIPAA security regulations about integrity, covered entities must formulate policies and take measures to protect personal health data against inappropriate manipulation or destruction [46]. Digital signing is a very useful tool for ensuring the accuracy and integrity of data [47, 48]. The use of terminology systems when exchanging data also ensures integrity [27, 49]. Both these mechanisms achieved expert agreement as integrity requirements in the present study.

To improve security and privacy, PHRs should implement access control, which includes authentication and authorization [8]. Authentication and authorization are other methods to assure the security of information systems. Authentication ensures that no unauthorized user can log into the system, and authorization guarantees that no user can access unauthorized resources by mistake [50, 51]. The most common authentication mechanisms in health records include the use of usernames and passwords [52] that achieved agreement in the present study, along with biometric scans (fingerprints, face, hands, retina).

Dimitropoulos [53] and HIPAA [54] mention “defining access levels and the role of authorized users to access information” as an authorization mechanism. Herein, this mechanism and “compiling a list of users who can access information in emergencies” were confirmed by experts. Chaudhary et al. noted that non-repudiation prevents users from denying that they have accessed or manipulated documents [35]. The National Committee on Vital and Health Statistics (NCVHS) hails audit log creation as a principle of non-repudiation [34]. According to Dalglish and Archer, the audit function is essential to compile a list of users who have accessed PHR data, so that unauthorized defects in information can be detected [23]. Similarly, in the current study, “creating an audit log” and “users' responsibility for any modification or manipulation” achieved expert agreement.

In PHRs, patients have the right to control their data and authorize access to/addition of information. The owner of data can authorize or reject access to all/part of the data to all/some users [31]. In line with this study, the Markle Foundation's Personal Health Technology Council declares that owners should have the right to assign the users who can access their PHRs, set the time of access, authorize other individuals to control this access and sharing of information, and view different entities' access to their information [27]. Also, Park et al. stated providers can obtain information from PHRs only when authorized through access controls set by the PHR owner [55].

## Conclusion

In integrated PHRs, people can access and control their health information at any time, from any place, and on any computer to participate in their healthcare. The wide adaptation and implementation of PHR can confer advantages, e.g., reducing healthcare costs, improving the quality of care, and achieving better health outcomes. The two distinct groups who have the greatest interest in creating and maintaining Personal Health Records (PHRs) are consumers (patients and their caregivers or healthy individuals) and healthcare providers (physicians or hospitals). Other stakeholders who have a stake in PHRs may include payers, employers, organizations, government, and health insurance companies. But security and privacy concerns have a seriously negative effect on the use intention of PHR by these stakeholders. The security requirements and mechanisms identified in this study can be used by system designers, health policy-makers, and healthcare organizations to design a reliable PHR. These requirements can be used in future studies to develop, implement and evaluate health records and information systems. Also, modern technologies are used to achieve these requirements which can be the subject of future studies.

## Abbreviations

PHRs	Personal Health Records
EHR	Electronic Health Record
HIPAA	Health Insurance Portability and Accountability Act
AHIMA	American Health Information Management Association
ISO	International Organization for Standardization
HL7	Health Level 7
NCVHS	National Committee on Vital and Health Statistics

## Supplementary Information

The online version contains supplementary material available at <https://doi.org/10.1186/s12911-023-02225-0>.

Supplementary Material 1

## Acknowledgements

This study was part of a Ph.D. project conducted at Shahid Beheshti University of Medical Sciences (Tehran, Iran).

## Authors' contributions

A.H., H.E., and S.P. were involved in concept and design, data acquisition, cleaning, and interpretation of data, and data analysis. S.P. and Y.S. have involved in drafting the manuscript. All authors were involved in critically revising the manuscript for important intellectual content. A.H. and H.E. were involved in supervision. All authors take responsibility for the final, published version and are accountable for all aspects of the work.

## Funding

None.

## Data availability

The data used and/or analyzed during the current study are available from the corresponding author upon reasonable request.

## Declarations

### Ethics approval and consent to participate

The study was approved by the Ethical Committee of the Shahid Beheshti University of Medical Sciences (IR.SBMU.RETECH.REC.1396.825). Participation in the study was voluntary. All participants were informed about the pertinent study aspects and provided written informed consent. All methods were performed in accordance with the relevant guidelines and regulations. Moreover, the participant's personal data is protected.

### Consent for publication

Not applicable.

### Competing interests

The authors declare no competing interests.

Received: 25 September 2022 / Accepted: 3 July 2023

Published online: 10 July 2023

## References

1. Chapman R, Haroon S, Simms-Williams N, Bhala N, Miah F, Nirantharakumar K, et al. Socioeconomic deprivation, age and language are barriers to accessing personal health records: a cross-sectional study of a large hospital-based personal health record system. *BMJ Open*. 2022;12(1):e054655. <https://doi.org/10.1136/bmjopen-2021-054655>.
2. Groenen CJ, Kremer JA, Int'Hout J, Meifroshan A, Niazkhani Z, Vandenbussche FP. Effects of a Personal Health Record in Maternity Care: a stepped-wedge trial. *Int J Environ Res Public Health*. 2021;18(19):10343. <https://doi.org/10.3390/ijerph181910343>.
3. Nahm E-S, Diblasi C, Gonzales E, Silver K, Zhu S, Sagerian K, et al. Patient-centered personal health record and portal implementation toolkit for ambulatory clinics: a feasibility study. *CIN: Comput Inform Nurs*. 2017;35(4):176–85. <https://doi.org/10.1097/CIN.0000000000000318>.
4. Toni E, Pirnejad H, Makhdoomi K, Mivefroshan A, Niazkhani Z. Patient empowerment through a user-centered design of an electronic Personal Health record: a qualitative study of user requirements in chronic kidney disease. *BMC Med Inform Decis Mak*. 2021;21:1–15. <https://doi.org/10.1186/s12911-021-01689-2>.
5. Vachon E, Robb BW, Haggstrom DA. Impact of a Personal Health record intervention upon Surveillance among Colorectal Cancer Survivors: Feasibility Study. *JMIR cancer*. 2022;8(3):e34851. <https://doi.org/10.2196/34851>.
6. Paydar S, Emami H, Asadi F, Moghaddasi H, Hosseini A. Functions and outcomes of personal health records for patients with chronic diseases: a systematic review. *Perspect Health Inf Manag* 2021, 18(Spring).
7. Alawneh R, El Sheikh A, Kanaan R. Development of embedded Personal Health Care Record System. *iBusiness*. 2011;3(2):178–83. <https://doi.org/10.4236/ib.2011.32024>.
8. Harahap NC, Handayani PW, Hidayanto AN. Functionalities and issues in the implementation of personal health records: systematic review. *JMIR*. 2021;23(7):e26236. <https://doi.org/10.2196/26236>.
9. Harahap NC, Handayani PW, Hidayanto AN. The Challenges in Integrated Personal Health Record Adoption in Indonesia: A Qualitative Analysis of Regulatory Perspectives. In: 2021 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS: 2021: IEEE; 2021: 169–174. <https://doi.org/10.1109/ICIMCIS53775.2021.9699353>.
10. Alkhatlan H. Evaluation of young adults' Preferences, needs, and the understandability of the Personal Health Record Data contents. University of Pittsburgh; 2010.
11. Caligtan CA, Dykes PC. Electronic health records and personal health records. In: *Seminars in oncology nursing*: 2011: Elsevier; 2011: 218–228. <https://doi.org/10.1016/j.soncn.2011.04.007>.
12. AHIMA e-HIM Personal Health Record Work Group. Defining the personal health record. *Journal of AHIMA* 2005, 76(6):24–25.2005.
13. Taha J, Czaja SJ, Sharit J, Morrow DG. Factors affecting usage of a personal health record (PHR) to manage health. *Psychol Aging*. 2013;28(4):1124. <https://doi.org/10.1037/a0033911>.
14. Andrikopoulou E, Scott P, Herrera H, Good A. What are the important design features of personal health records to improve medication adherence for

- patients with long-term conditions? A systematic literature review. *BMJ open*. 2019;9(9):e028628. <https://doi.org/10.1136/bmjopen-2018-028628>.
15. Bourgeois FC, Nigrin DJ, Harper MB. Preserving patient privacy and confidentiality in the era of personal health records. *Pediatrics*. 2015;135(5):e1125–7. <https://doi.org/10.1542/peds.2014-3754>.
  16. Abd-Alrazaq A, Bewick BM, Farragher T, Gardner P. Factors affecting patients' Use of Electronic Personal Health Records in England: cross-sectional study. *JMIR*. 2019;21(7):e12373. <https://doi.org/10.2196/12373>.
  17. Flaumenhaft Y, Ben-Assuli O. Personal health records, global policy and regulation review. *Health Policy*. 2018;122(8):815–26. <https://doi.org/10.1016/j.healthpol.2018.05.002>.
  18. Fylan F, Caveney L, Cartwright A, Fylan B. Making it work for me: beliefs about making a personal health record relevant and useable. *BMC Health Serv Res*. 2018;18(1):1–12. <https://doi.org/10.1186/s12913-018-3254-z>.
  19. Kaelber DC, Jha AK, Johnston D, Middleton B, Bates DW. A research agenda for personal health records (PHRs). *J Am Med Inform Assoc*. 2008;15(6):729–36. <https://doi.org/10.1197/jamia.M2547>.
  20. Dontje K, Corser WD, Holzman G. Understanding patient perceptions of the electronic personal health record. *J Nurse Pract*. 2014;10(10):824–8. <https://doi.org/10.1016/j.nurpra.2014.09.009>.
  21. Hawthorne KH, Richards L. Personal health records: a new type of electronic medical record. *Records Manage J*. 2017. <https://doi.org/10.1108/RMJ-08-2016-0020>.
  22. Pang PC-I, McKay D, Chang S, Chen Q, Zhang X, Cui L. Privacy concerns of the Australian My Health Record: implications for other large-scale opt-out personal health records. *Inf Process Manag*. 2020;57(6):102364. <https://doi.org/10.1016/j.ipm.2020.102364>.
  23. Daglish D, Archer N. Electronic personal health record systems: a brief review of privacy, security, and architectural issues. In: *Privacy, Security, Trust and the Management of e-Business*, 2009 CONGRESS'09 World Congress on: 2009: IEEE; 2009: 110–120. <https://doi.org/10.1109/CONGRESS.2009.1>.
  24. Furano RF, Kushniruk AW, Barnett J. Deriving a Set of Privacy Specific Heuristics for the Assessment of PHRs (Personal Health Records). In: *ITCH: 2017*; 2017: 125–130. <https://doi.org/10.3233/978-1-61499-742-9-125>.
  25. Meigasari DA, Handayani PW, Hidayanto AN, Ayuningtyas D. Do Electronic Personal Health Records (E-PHR) Influence People Behavior to Manage Their Health? In: 2020 International Conference on Information Management and Technology (ICIMTech): 2020: IEEE; 2020: 482–487. <https://doi.org/10.1109/ICIMTech50083.2020.9211293>.
  26. Farzandipour M, Sadoughi F, Ahmadi M, Karimi I. Security requirements and solutions in electronic health records: lessons learned from a comparative study. *J Med Syst*. 2010;34(4):629–42. <https://link.springer.com/article/10.1007/s10916-009-9276-7>.
  27. US Department of Health Human Services. Literature review and environmental scan: evaluation of personal health records pilots for fee-for-service Medicare enrollees from South Carolina. 2010, 17:2012.
  28. Wynia M, Dunn K. Dreams and nightmares: practical and ethical issues for patients and physicians using personal health records. *J Law Med Ethics*. 2010;38(1):64–73. <https://doi.org/10.1111/j.1748-720X.2010.00467.x>.
  29. Rodolfo I, Laranjo L, Correia N, Duarte C. Design strategy for a national integrated personal health record. In: *Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational*: 2014; 2014: 411–420. <https://doi.org/10.1145/2639189.2641205>.
  30. Rodolfo IMS. Design strategy for Integrated Personal Health Records: improving the user experience of Digital Healthcare and Wellbeing. Universidade NOVA de Lisboa (Portugal); 2017.
  31. Alyami MA. Toward patient-centered personal health records systems to promote evidence-based decision-making and information sharing. *Towson University*; 2018.
  32. Abdekhoda M, Dehnad A, Khezri H. The effect of confidentiality and privacy concerns on adoption of personal health record from patient's perspective. *Health and Technology*. 2019;9(4):463–9. <https://doi.org/10.1007/s12553-018-00287-z>.
  33. Kumar N, Mathuria A. Security and privacy issues in outsourced Personal Health Record. *Research advances in Cloud Computing*. Springer; 2017: 431–47. [https://doi.org/10.1007/978-981-10-5026-8\\_17](https://doi.org/10.1007/978-981-10-5026-8_17).
  34. Israelson J, Cankaya EC. A hybrid web based personal health record system shielded with comprehensive security. In: *System Science (HICSS)*, 2012 45th Hawaii International Conference on: 2012: IEEE; 2012: 2958–2968. <https://doi.org/10.1109/HICSS.2012.6>.
  35. Chaudhary S, Somani G, Buyya R. *Research advances in Cloud Computing*. Springer; 2017. <https://doi.org/10.1007/978-981-10-5026-8>.
  36. Padol PR, More HK, Mandre NV, Shimpi PN. Personal health records in cloud computing. *Int Res J Eng Technol*. 2018;5(2):1666–73.
  37. Señor IC, Fernández-Alemán JL, Toval A. Are personal health records safe? A review of free web-accessible personal health record privacy policies. *JMIR*. 2012;14(4):e114. <https://doi.org/10.2196/jmir.1904>.
  38. Wang C-K. Security and privacy of personal health record, electronic medical record and health information. *Probl Perspect Manage*. 2015;13(4):19–26.
  39. Kyriazis D, Autexier S, Boniface M, Engen V, Jimenez-Peris R, Jordan B et al. The CrowdHEALTH project and the holistic health records: collective wisdom driving public health policies. *Acta Inf Med* 2019, 27(5):369. <https://doi.org/10.5455/aim.2019.27.369-373>.
  40. Kiourtis A, Mavrogiorgou A, Mavrogiorgos K, Kyriazis D, Graziani A, Symvoulidis C, et al. Electronic Health Records at People's Hands across Europe: the InteropEHRate Protocols. In: *pHealth 2022*. IOS Press; 2022. pp. 145–50. <https://doi.org/10.3233/SHI220973>.
  41. Hansen A. Guidelines on Minimum/Non-Exhaustive patient Summary dataset for Electronic Exchange in Accordance with the Cross-Border Directive 2011/24. In: *European Commission*; 2013.
  42. Samarati P, de Vimercati SC. Access control: Policies, models, and mechanisms. In: *International School on Foundations of Security Analysis and Design*: 2000: Springer; 2000: 137–196. [https://doi.org/10.1007/3-540-45608-2\\_3](https://doi.org/10.1007/3-540-45608-2_3).
  43. Abdulnabi M, Al-Haiqi A, Kiah MLM, Zaidan A, Zaidan B, Hussain M. A distributed framework for health information exchange using smartphone technologies. *J Biomed Inform*. 2017;69:230–50. <https://doi.org/10.1016/j.jbi.2017.04.013>.
  44. Coatrieux G. Contribution au contrôle d'intégrité des images médicales. Université de Rennes 1; 2011.
  45. Zhou L, DeAlmeida D, Parmanto B. Applying a user-centered approach to building a mobile personal health record app: development and usability study. *JMIR mHealth and uHealth*. 2019;7(7):e13194. <https://doi.org/10.2196/13194>. <https://preprints.jmir.org/preprint/13194>.
  46. Avancha S, Baxi A, Kotz D. Privacy in mobile technology for personal healthcare. *ACM Comput Surv (CSUR)*. 2012;45(1):1–54. <https://doi.org/10.1145/2379776.2379779>.
  47. Blobel B. Architectural approach to eHealth for enabling paradigm changes in health. *Methods Inf Med*. 2010;49(2):123–34. <https://doi.org/10.3414/ME9308>.
  48. Romero J, López P, Noguera JLV, Cappo C, Pinto-Roa DP, Villalba C. Integrated, reliable and cloud-based personal health record: a scoping review. *arXiv preprint arXiv*. 2016;160903615. <https://doi.org/10.48550/arXiv.1609.03615>.
  49. Dubbink D. Personal health records in dutch hospitals: is hte hype already over? University of Twente; 2013.
  50. Keikavousi MR, Asadi F, Paydar S, Khounraz F. Development of Inflammatory Bowel Diseases Registry Software. *Middle East J Dig Dis* 2021, 13(2):145. <https://doi.org/10.34172/mejdd.2021.218>.
  51. Mishra P. User interface design: for existing system monitoring application. 2013.
  52. Fernández-Alemán JL, Señor IC, Lozoya PÁO, Toval A. Security and privacy in electronic health records: a systematic literature review. *J Biomed Inform*. 2013;46(3):541–62. <https://doi.org/10.1016/j.jbi.2012.12.003>.
  53. Dimitropoulos LL. Privacy and security solutions for interoperable health information exchange. *Impact analysis*. RTI International; 2007.
  54. US Department of Health and Human Services. Personal health records and the HIPAA privacy rule. Washington, [accessed 2020-06-20][WebCite Cache ID 6kLwH4Pzu]. 2008. DC URL: <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/healthit/phrs.pdf>.
  55. Park HS, Kim KI, Soh JY, Hyun YH, Jang SK, Lee S, et al. Factors influencing acceptance of personal health record apps for workplace health promotion: cross-sectional questionnaire study. *JMIR mHealth and uHealth*. 2020;8(6):e16723. <https://doi.org/10.2196/16723>.

## Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.