“Security and privacy of personal health record, electronic medical record and health information”

AUTHORS	Cheng-Kun Wang
ARTICLE INFO	Cheng-Kun Wang (2015). Security and privacy of personal health record, electronic medical record and health information. *Problems and Perspectives in Management*, *13*(4), 19-26
RELEASED ON	Tuesday, 15 December 2015
JOURNAL	"Problems and Perspectives in Management"
FOUNDER	LLC “Consulting Publishing Company “Business Perspectives”

NUMBER OF REFERENCES	NUMBER OF FIGURES	NUMBER OF TABLES
0	0	0

Cheng-Kun Wang (Taiwan)

Security and privacy of personal health record, electronic medical record and health information

Abstract

Security and privacy are two crucial issues in the protection of health information. The purpose is to keep the medical privacy of confidential information about the patient. The successful implementation and application of electronic medical record (EMR), electronic health record (EHR) and personal health record (PHR) prove to be a difficult task, due to a mixture of technical, organizational and political issues. By analyzing 13,960 citations of 410 articles published in SSCI (Social Science Citation Index) and SCI (Science Citation Index) journals about the privacy and security of health information from 2004 to 2013, the author plotted virtual social networks between researchers. The interpretation of result is that privacy and security of health information between 2009-2013 included at least 6 subfields: personal health records, HIPAA privacy rule, authentication, protecting health privacy, encryption and electronic health records. Electronic health information system designer must prevent unauthorized use and hacker attacks. Authentication and cryptographic key management will become the tools of choice for protecting privacy and security. The author combines quantitative bibliometrics and qualitative literature reviews to find out the important articles about security and privacy for health information, and realize the relationship between important topics in this field. When the patients trust in health information network is secure, it would improve the implementation of PHR. The dimension of trust can be divided into trust of physicians and trust of patients. Future researches could adopt "trust" as an independent variable for health information research and to find the relationship between protection of "security and privacy" of PHR and "trust".

Keywords: security, privacy, electronic medical records, personal health records, virtual social network, data mining.
JEL Classification: I1.

Introduction

Electronic medical records' (EMRs) technological innovation is considered to be a key factor to ease the burdens of health care. Therefore, the EMR is considered to be a technology-driven core component in the reform process. However, the successful implementation and adoption of electronic medical records system proved to be a difficult task, due to the mixed technical, organizational and political issues (Emmanouilidou & Burke, 2013). An electronic health record (EHR) or electronic medical record (EMR), is a systematic collection of electronic health information about an individual patient or population. A personal health record (PHR) is a health record where health data related to the care of a patient is maintained by the patient (Tang, Ash, Bates, Overhage & Sands, 2006). Electronic PHR system support patient-centered medical care in health self-management to make medical records and other relevant information are accessible to patients (Archer, Fevrier-Thomas, Lokker, McKibbon & Straus, 2011).

Privacy and security are two crucial issues in the protection of health information (Lee & Lee, 2008). Privacy must be protected in the business of medical information technology systems. Protection must include the ability to consent to care, agreed to release care-related information, and prevent inadvertent disclosure through billing activities or electronic aggregation of data for quality improvement, research, public health reporting or other purposes (Blythe et al., 2012). Security issues must be addressed differently, and hence new security challenges are raised. The information system design needs the integration of many technologies such as: computers, smart meters, sensing devices, mobile devices, RFID, Wi-Fi network, Low-Power Personal Area Networks, cellular network. Designers should adopt new security design solutions to ensure privacy and data confidentiality (Saleem, Derhab, Al-Muhtadi & Shahzad, 2014).

Medical privacy can also refer to the interaction between patients and providers while in a medical facility. Many concerns include the degree of disclosure to insurance companies, employers and other third parties. The emergence of EHRs has raised new concerns about privacy, balancing efforts to reduce duplication of medical records and medical errors. Electronic health information system of designer must protect health information.

Bibliometric analysis of articles was adopted popularly. Wagstaff took a bibliometric tour of the last forty years of health economics. They used bibliographic "metadata" from EconLit supplemented by citation data from Google Scholar, and to report the development of health economics (Wagstaff & Culyer, 2012). By co-citation analysis and bibliometric analysis, we found privacy and security were the hot issues in many health

Cheng-Kun Wang, Graduate School of Business and Operations Management, Chang Jung Christian University, Tainan City, Taiwan.

information papers. Many authors provided methods to improve the security of health information and protect the privacy of PHR. When many information security disasters appeared, many researchers provide methods to protect information system.

1. Theoretical development

There are a number of techniques that can be used to study a body of literature. Most frequent is the simple literature review where a highly subjective approach is used to structure the earlier work. Objective and quantitative techniques have recently become popular with more databases available online for use (Wang, McLee & Kuo, 2011). If I have seen further, it is by standing on the shoulders of giants (Sir Issac Newton, 1645-1736). It's said "stand on the shoulders of giants (the under-box slogan of Google Scholar®)" in which giants means the highly cited authors, papers and books. The highly cited authors, papers and books could help a novice to navigate the blue ocean of knowledge domain when the novice knows nothing (Etemad & Lee, 2003).

We use the citation analysis to draw the development timeline, and use co-citation analysis to predict the future development of health care development and to know how it works. Bibliometrics can be a powerful research methodology for the understanding the epistemology of a field as it has evolved (and continues to evolve) by providing a historical timeline to follow up. Bibliometrics with quantitative analysis is applied to analyze many articles's citation data and realize the paradigm shift of this field.

Every discipline could be seen as a particular knowledge system that is a component of a more general knowledge system. Within each discipline, journal articles, books, and monographs fill the fundamental role of storing and distributing information. Of these three means of formal communication, journal articles are perhaps the most competitive and controversial. Consequently, citations that appear in journal articles published in the journals of a particular discipline provide an objective measure of the contributions of the development and progress of that particular discipline. Citations also give a relative measure of the particular contributions of authors, articles, and journals. This analysis reveals a wealth of information, for example the lists of highly-cited authors, books, and articles presented here.

2. Methods

In this study, well-recognized high-quality database of SSCI (Social Science Citation Index) and SCI (Science Citation Index) were adopted. First, we used the bibliometric analysis to find out the quantity of hot papers, hot authors and hot key words. Second, we adopted social network analysis to identify popular issues that were interesting for many researchers. Finally, critical qualitative literature review was performed and found the solution for the problem about security and privacy in health information.

We adopted the citation analysis to study privacy and security of health information between 2004 and 2013. We searched the terms "privacy", "security" and "health" in journals listed in the SSCI and SCI database. We selected the top-ranking papers (times-cited ranking, highly-cited ranking) in each five-year period (2004-2008, 2009-2013). Finally, we analyzed 13,960 citations of 410 articles in the period 2004-2013. The citation data used in this study includes journal articles, authors, keywords, and cited references. Some articles were highly cited. The frequency of citation (times cited) reveal the importance of this article. The most influential article is the highly-cited article.

One paper cited two different authors in the same time was called the "co-citation". There were some relationship between these two different authors. Virtual social networks meant these two authors even without contacting with the other one, but they did similar research in the field, so these two authors could produce a link in the virtual social network. Citation and co-citation analysis is the main method for this study. First, the SCI and SSCI database were identified as the sources of privacy and security of health publications. Then data collection and analysis techniques were designed to collect information about topics on privacy and security of health research. The collected data were analyzed and systematized by sorting, screening, summing, sub-totalling, and ranking. The data were run by the UCINET software (Borgatti, Everett & Freeman, 2002). After a series of operations, the co-citation analysis revealed the virtual social networks of privacy and security of health information.

Co-citation analysis is a bibliometric technique. It involves counting documents from a chosen field-paired or co-cited documents. Co-citation analysis compiles co-citation counts in matrix form and statistically scales them to capture a snapshot at a distinct point in time of what is actually a changing and evolving structure of knowledge (Small, 1993).

Co-citations were tabulated for each source documents by using the Excel package. Some authors were too new to had time to impact on the literature. Based on the total number of citations in the selected journals, the top scholars were identified, and then a co-citation matrix was built before a pictorial map was drawn. The map of relationship of authors describes the correlations among different scholars. In doing so, we were following the procedures recommended by White and Griffith (Garfield & Merton, 1979). We adopted factor analysis to distinguish the groups of authors between different factions.

3. Results

After analyzing the 13,960 citations of 410 articles published in SSCI and SCI journals on privacy and security in the health field from year 2004 to year 2013, a timeline of the most highly cited authors and papers was developed. The detailed data included 4,331 citations of 137 articles from year 2004 to year 2008, and 9,629 citations of 273 articles from year 2009 to year 2013.

3.1. Citation analysis and timeline. Table 1 shows the historical timeline of privacy and security issues by bibliometrics analysis. The frequency of citation (times cited) indicates the importance of the article. The most influential article is assumed to be the most frequently cited. The security of health information field is an emerging topic, so there is not many citations of articles. Some articles were highly cited. The frequency of citation (times cited) reveal the importance of this article. The most influential article is the highly-cited article.

Table 1. Timeline of privacy and security in health articles (citations from SSCI and SCI articles, 2009-2013)

Year	Frequency of citation/times cited	B/J*	Author	Article			
1979	7	J	Shamir, A.	1979	Communications of the ACM	v 22	p. 612
1996	8	J	Barrows, R.C.	1996	Journal of the american medical informatics association	v 3	p. 139
2001	6	B	Institute of medicine	2001	Crossing the quality chasm		
2002	15	J	Sweeney, L.	2002	International journal of uncertainty, fuzziness and knowledge-based systems	v 10	p. 557
2002	7	J	Kim Mi	2002	Journal of the american medical informatics association	v 9	p. 171
2003	6	B	Cherukuri, S.	2003	Parallel processing workshops, 2003. Proceedings. 2003 international conference on. IEEE		
2004	6	J	Blobel, B.	2004	International journal of medical informatics	v 73	p. 251
2004	6	J	Lorincz, K.	2004	Pervasive computing, IEEE	v 3	p. 16
2006	14	J	Tang, P.C.	2006	Journal of the american medical informatics association	v 13	p. 121
2006	10	J	Poon, C.C.Y.	2006	Communications magazine, IEEE	v 44	p. 73
2006	7	J	Blobel, B.	2006	International journal of medical informatics	v 75	p. 597
2006	7	J	Yang, C.M.	2006	Computer methods and programs in biomedicine	v 82	p. 277
2006	6	J	Whiddett, R.	2006	International journal of medical informatics	v 75	p. 530
2006	6	J	Chaudhry, B.	2006	Annals of internal medicine	v 144	p. 742
2007	7	J	Safran, C.	2007	Journal of the american medical informatics association	v 14	p. 1
2007	6	J	Ralston, J.D.	2007	Journal of the american medical informatics association	v 14	p. 798
2007	6	J	Sucurovic, S.	2007	International journal of medical informatics	v 76	p. 491
2007	6	J	Agrawal, R.	2007	International journal of medical informatics	v 76	p. 471
2008	10	J	Kaelber, D.C.	2008	Journal of the american medical informatics association	v 15	p. 729
2008	9	J	Lee, W.B.	2008	Information technology in biomedicine, IEEE transactions	v 12	p. 34
2008	6	J	Steinbrook, R.	2008	New england journal of medicine	v 358	p. 1653
2008	6	J	Halamka, J.D.	2008	Journal of the american medical informatics association	v 15	p. 1
2008	6	J	Desroches, C.M.	2008	New england journal of medicine	v 359	p. 50
2008	6	J	Halperin, D.	2008	Pervasive computing, IEEE	v 7	p. 30
2009	8	J	Van Der Linden, H.	2009	International journal of medical informatics	v 78	p. 141
2009	8	J	Mcgraw, D.	2009	Health affairs	v 28	p. 416
2009	7	J	Kahn, J.S.	2009	Health affairs	v 28	p. 369
2009	6	J	Simon, S.R.	2009	Journal of medical internet research	v 11	doi 10.2196/jmir.1164
2009	6	J	Lin, X.D.	2009	IEEE Journal on Selected Areas in Communications	v 27	p. 365
2009	6	J	Jha, A.K.	2009	New england journal of medicine	v 360	p. 1628
2009	6	J	Tripathi, M.	2009	Health affairs	v 28	p. 435
2010	7	J	Brown, J.S.	2010	Medical care	v 48	p. 45
2010	6	J	Hu, J.K.	2010	Computer Standards & Interfaces	v 32	p. 274
2012	6	J	He, D.B.	2012	Journal of medical systems	v 36	p. 1989

Note: B/J: B: book, J: journal.

Sweeney, shown with fifteen citations in Table 1, presented a protection model for the privacy of personal data in 2002, considered a data holder, such as a hospital or a bank, which has a privately held collection of person-specific data. Assuming the data holder wants to share a version of the data with researchers. How can it be that data holder release a version of one's private data with scientific guarantees, and the individuals who are the subjects of the data cannot be re-identified but the data can still remain useful? (Sweeney, 2002).

Kaelber, shown with 10 citations in Table 1, focused a paper in 2008 on the research agenda for personal health records and mentioned related issues of privacy and security (Kaelber, Jha, Johnston, Middleton & Bates, 2008). In 2009, Kahn focused on characteristics of the ideal personal health record. Privacy is part of a complex problem because new PHRs are not necessarily covered by the HIPAA regulations. An important policy implication is to protect online health information and develop the tools for secure data exchange (Kahn, Aulakh & Bosworth, 2009). In 2010, Brown focused on distributed health data networks (Brown et al., 2010). Telecare is the term for offering remote care of people, providing the care and reassurance needed to allow them to remain living in their own homes. The use of sensors may be part of a package which can provide help for people with illnesses. In 2012, Debiao focused on a more secure authentication scheme for telecare medicine information systems (Debiao, Jianhua & Rui, 2012).

3.2. Key words ananlysis. Keywords analysis can give researchers a direction to find the hot research topics. Table 2 shows the keyword analysis of 410 articles published in SSCI and SCI journals. There is some increase in the frequency of some emerging keywords. Comparison of keyword analysis between the two five-year periods (2004-2008 and 2009-2013) revealed that care, privacy, technology, security, confidentiality, records, communication, access-control, design and internet are the emerging topics.

Table 2. Analysis of keywords of 410 articles between two five-year periods

Years 2004-2008		Years 2009-2013		Obvious increase (+)
Keyword	Frequency	Keyword	Frequency	
security	19	care	36	+
information	14	privacy	31	+
privacy	13	technology	22	+
care	13	security	22	+
systems	11	systems	16	
health	11	health	15	
quality	8	information	14	
technology	7	confidentiality	14	+
internet	5	health care	12	
primary care	5	records	12	+
information systems	4	communication	11	+
health information	4	management	11	
medical records	4	access control	10	+
management	4	information systems	9	
confidentiality	4	design	9	+
access	4	internet	9	+
records	3	model	8	
system	3	implementation	8	
genera practice	3	quality	8	

3.3. Co-citation analysis. One paper cited two different authors in the same time was called the "co-citation". There was some relationship between these two different authors. We adopted factor analysis to distinguish the groups of authors between different faction. Virtual social network analysis techniques were used to plot the relationships in the co-citation matrix. We identified the strongest links and the core areas of the authors. Different linkage would appear after performing a "faction study" of these authors (Wang et al., 2011). This method seeks to group elements in a network based on the sharing of common links to each other. By taking co-citation matrix and adopting factor analysis, the correlation between the authors were analyzed. When authors are grouped together, there are common elements between the grouped authors. According to this analysis, the closeness of these authors revealed their algorithmically similar perception perceived by citers (Wang et al., 2011). The co-citation correlation matrix was factor-analyzed with varimax rotation, a commonly used procedure that attempts to fit (or load) the maximum number of authors on the minimum number of factors (McCain, 1990).

Table 3. Author factor loadings: years 2009-2013

Year 2009-2013		Name of group			Name of group
Factor 1	Variance	Personal health records	Factor 2	Variance	HIPAA privacy rule
Bao, S.D.	0.956		Agrawal, R.	0.934	
Sweeney, L.	0.934		Malin, B.	0.815	
Tang, P.C.	0.667		El Emam, K.	0.634	
Jha, A.K.	0.548				
Li, M.	0.543				
Factor 3	Variance	Authentication	Factor 4	Variance	Protecting health privacy
Sufi, F.	0.888		Li, M.	0.857	
Venkatasubramanian, K.	0.813		Rothstein, M.A.	0.768	

Table 3 (cont.). Author factor loadings: years 2009-2013

Year 2009-2013		Name of group			Name of group
Poon, C.C.Y.	0.802	Authentication	Mcgraw, D.	0.685	Protecting health privacy
Bao, S.D.	0.578		Mandl, K.D.	0.541	
Factor 5	Variance	Encryption	Factor 6	Variance	Electronic health records
Boneh, D.	0.893		Jha, A.K.	0.938	
He, D.B.	0.687		Steinbrook, R.	0.894	
			Tang, P.C.	0.546	

Six factors were extracted from the data between 2009 and 2013; together they explained over 68.4% of the variance in the correlation matrix. Table 3 lists the six most important factors along with the authors that had a factor loading of at least 0.5. As is usual in this type of analysis, authors with less than a 0.5 loading or with cross-loadings were dropped from the final results (White & Griffith, 1981). We tentatively assigned names to the factors on the basis of our own interpretation of the authors with high loadings. Our interpretation of the analysis results is that privacy and security of health information between year 2009-2013 is composed of at least six different sub-fields: personal health records, HIPAA privacy rule, authentication, protecting health privacy, encryption and electronic health records (see Table 3). We made no attempt to interpret the remaining factors due to their small eigenvalues.

4. Discussion

After analyzing each paper's citations information, we can find the hot papers and authors. We adopt citation statistics to find the important cited papers. They revealed in Table 1 as frequency of citation. With literature review of the hot papers, we can understand the implication of security and privacy of health information. A literature review includes the current knowledge, as well as theoretical and methodological contributions to a particular topic. Literature reviews use secondary sources, and do not report new or original experimental work. It helps us to understand the whole picture of security and privacy of health information.

After co-citation analysis was performed, the virtual social network appeared. The factor analysis revealed several factions of researchers in different topics. The linked researchers focused on some topics, such as personal health records, HIPAA privacy rule, authentication, protecting health privacy, encryption and electronic health records. When the electronic medical records and cloud database become more popular, people pay attention to the importance about privacy and security of health information.

5. Literature reviews after citation analysis

The qualitative literature review of hightly cited papers provokes critical thinking of about electronic health records. In 2004, Blobel focused on authorization and access control for electronic health record systems. To enhance personal health information, the basic concepts related to security and safety, aggregations, networks of relationships and business ideas must be specified and modelled by international experts in the field (Blobel, 2004). The issue of PHR was widely discussed in the literature. Web-based applications of PHR allow patients to enter their own information into secure personal health records. PHR's future development should be guided by patient-oriented research targeted to evaluate the performance and usability of evolving applications (Kim & Johnson, 2002). Patient-oriented web services integrated with a shared medical record is the trend of development. Web services integrated with clinical information systems and patient-provider relationships may be important in meeting the needs of patients (Ralston et al., 2007). In 2012, Señor revealed that most privacy protection policies of PHR systems do not provide an in-depth description of the security measures they use. In addition, compliance with standards and regulations of PHR system is still low (Señor, Fernández-Alemán, & Toval, 2012). The barriers of PHR adoption were that the providers fear for illegal problems and the individuals fear for privacy concerns (Tang et al., 2006). The faster adoption of EHR to assess quality is valuable (Blumenthal & Dixon, 2012).

Personal health record (PHR) adoption is dependent on growth in electronic health records (EHR) adoption. Many PHR systems are physician-oriented, do not include patient-oriented features. PHR adoption has many barriers. As with any new technology, the failure can often be linked to a lack of planning, design and implementation of consumer participation. Lack of provider's trust is another obstacle, as are poor computer and internet skills, fear of technology, inadequate access, low health literacy and limited physical and cognitive abilities (Archer et al., 2011). Patients, policymakers, providers, payers, employers and others have an increasing interest in using PHR systems to improve healthcare costs, quality and efficiency. However, patients are most concerned about almost all types of electronic healthcare applications, including the PHR, is the privacy and security (Kaelber et al., 2008).

Privacy and security issues in healthcare apply to both paper and electronic medical records. Breaches in so-called secure data at centralized data repositories in banking and other financial institutions were noted by government. Therefore, government pays attention to the security and privacy of electronic medical records. Records that are exchanged over the internet are subject to the same security issues as any other type of data transaction in the medium. The Health Insurance Portability and Accountability Act (HIPAA) established rules for access, authentication, storage, auditing and transmittal of electronic medical records. These standards for electronic records have more stringent restrictions than paper records. However, there are concerns as to the adequacy of the standards (Wafa, 2010).

Encryption mechanism is well defined to provide appropriate solutions of protection for privacy and security of PHR. A cryptographic key management solution for privacy and security regulations was proposed (Lee & Lee, 2008). User authentication techniques have been widely deployed in various applications, such as remote login, withdrawals from automatic teller machines, and physical entry to restricted areas. Some improved password authentication scheme was developed to withstand the impersonation attack and the insider's attack (Debiao et al., 2012).

Distributed networks would obviate the need for centralized database, thus avoiding numerous obstacles. A distributed network can perform almost all the functions required for a centralized database, and avoids many of the disadvantages of the centralized database. They allow data holders to maintain physical control over their data. Distributed systems minimize the need for disclosure of protected health information to reduce patients' privacy concerns. Distributed networks can handle electronic healthcare data to meet nearly all the intended use (Brown et al., 2010).

Limitations

The citations used in this study are the voting behavior measurements of authors. But the citations are of old articles. Citation analysis can find the previous paradigm and paradigm shift, but some authors are too new to be cited. We cannot therefore identify the future important authors, but we can follow the research trend.

Conclusion

We combine quantitative bibliometrics and qualitative literature reviews to find out the important articles about privacy and security for health information, and realize the relationship between hot topics in this field. This study is to analyze the citation data of health articles, and identify the same themes of various researchers, and find out hot topics. We adopted bibliometric methods to generate quantitative data, then identify important issues of privacy and security of health information through subjective judgement. Finally, we adopted qualitative literature review to explore these important issues. The co-citation analysis produced several different factions of authors. The hot topics about privacy and security were discussed by authors of different factions. This is a mixed method of quantification and qualitative research. The qualitative literature review of highly cited papers provokes critical thinking of about privacy and security of health information.

Keywords are the meaningful vocabularies of papers. The keywords arranged in front were important themes. We choose some popular keywords subjectively after literature reviews. The hot keywords are as following: privacy, technology, security, confidentiality, records, access-control, design and internet during these periods. The important keywords revealed the privacy and security of health information are valuable.

Nowadays, hospitals and clinics adopt electronic medical records to store the patient's health data. The healthcare data are stored in computer and transmitted through internet. Some of health information is stored in cloud database. The electronic medical devices generate large amount of healthcare data transmitted to centralized database. Threats to health records can be categorized under three headings: (1) human threats, such as from employees or hackers. Man-made disasters may be intentional (for example, a terrorist act) or unintentional. (2) Natural and environmental disasters, such as flood, earthquakes, hurricanes and fires; and (3) technology failures such as computer system crashes. A disaster recovery planning can protect health records, that is a series of steps to restore and protect the information technology infrastructure in the event of a disaster. The organization is to follow the prescribed plans in the event of a disaster. Paying attention to cybersecurity can prevent hacker's attack through internet. Cybersecurity standards are security standards which enable organizations to practice safe security techniques to stop cyber-attack. These cybersecurity standards provide general outlines as well as specific techniques for implementing cybersecurity. If the disease records of some world leaders are stolen from the information system or cloud database, it will become a disaster. If the hackers can control the medical devices through internet, it will become dangerous. The protection of security and privacy of health information is very important.

The interpretation of the co-citation analysis revealed six hot topics: personal health records, HIPAA privacy rule, authentication, protecting health privacy, encryption and electronic health records. The relationship between the six themes is about the security and privacy. There is a need for policy-makers to develop policies to protect privacy and security of medical records and to enlist doctors' and patients' agreement to the use of electronic medical records. Program designer must prevent unauthorized use and hacker attacks, to protect medical records. Privacy principles assure that patients have more control over their health information and set limits on the use and disclosure of PHR. The principle of security is to protect data integrity, confidentiality and availability. Authentication and cryptographic key management will become the tools of choice for protecting privacy and security.

The rise of cloud computing and personal health databases becomes a global trend. The history of disease and real-time data about patient's respiratory rate and heartbeats have a great help for personal health care. If this health information is stolen, this would endanger the privacy and safety of patients. Many hackers had attacked many governments or banks. These information security risks threaten individual lives. After literature reviews, we find that the success of implementation of PHR must rely on the software engineering sector encryption, authorization, good data preservation and trust from patients and doctors. Lack of trust is another obstacle of implementation of PHR. When the patients trust in health information networks are secure, it would improve the implementation of PHR. The dimension of trust can be divided into trust of physicians and trust of patients. Future researches could adopt "trust" as an independent variable for health information research and to find the relationship between protection of "security and privacy" of PHR and "trust".

References

1. Archer, N., Fevrier-Thomas, U., Lokker, C., McKibbon, K. & Straus, S. (2011). Personal health records: A scoping review, *Journal of the American Medical Informatics Association*, 18 (4), pp. 515-522.
2. Blobel, B. (2004). Authorisation and access control for electronic health record systems, *International Journal of Medical Informatics*, 73 (3), pp. 251-258.
3. Blumenthal, D. & Dixon, J. (2012). Health-care reforms in the USA and england: Areas for useful learning, *The Lancet*, 380 (9850), pp. 1352-1357.
4. Blythe, M.J., Adelman, W.P., Breuner, C.C., Levine, D.A., Marcell, A.V., Murray, P.J., ... Weinberg, S.T. (2012). *Standards for health information technology to ensure adolescent privacy*, *Pediatrics*, 130 (5), pp. 987-990.
5. Borgatti, S.P., Everett, M.G. & Freeman, L.C. (2002). Ucinet for windows: Software for social network analysis.
6. Brown, J.S., Holmes, J.H., Shah, K., Hall, K., Lazarus, R. & Platt, R. (2010). Distributed health data networks: A practical and preferred approach to multi-institutional evaluations of comparative effectiveness, safety, and quality of care, *Medical Care*, 48 (6 Suppl), pp. 45-51.
7. Debiao, H., Jianhua, C. & Rui, Z. (2012). A more secure authentication scheme for telecare medicine information systems, *Journal of Medical Systems*, 36 (3), pp. 1989-1995.
8. Emmanouilidou, M. & Burke, M. (2013). A thematic review and a policy-analysis agenda of electronic health records in the greek national health system, *Health Policy*, 109 (1), pp. 31-37.
9. Etemad, H. & Lee, Y. (2003). The knowledge network of international entrepreneurship: Theory and evidence, *Small Business Economics*, 20 (1), pp. 5-23.
10. Kaelber, D.C., Jha, A.K., Johnston, D., Middleton, B. & Bates, D.W. (2008). A research agenda for personal health records (PHRs), *Journal of the American Medical Informatics Association*, 15 (6), pp. 729-736.
11. Kahn, J.S., Aulakh, V. & Bosworth, A. (2009). What it takes: Characteristics of the ideal personal health record, *Health Affairs*, 28 (2), pp. 369-376.
12. Kim, M.I. & Johnson, K.B. (2002). Personal health records evaluation of functionality and utility, *Journal of the American Medical Informatics Association*, 9 (2), pp. 171-180.
13. Lee, W.B. & Lee, C.D. (2008). *A cryptographic key management solution for HIPAA privacy/security regulations*, Information Technology in Biomedicine, IEEE Transactions On, 12 (1), pp. 34-41.
14. McCain, K.W. (1990). Mapping authors in intellectual space: A technical overview, *Journal of the American Society for Information Science*, 41 (6), pp. 433-443.
15. Ralston, J.D., Carrell, D., Reid, R., Anderson, M., Moran, M. & Hereford, J. (2007). Patient web services integrated with a shared medical record: Patient use and satisfaction, *Journal of the American Medical Informatics Association*, 14 (6), pp. 798-806.
16. Saleem, K., Derhab, A., Al-Muhtadi, J. & Shahzad, B. (2014). *Human-oriented design of secure machine-to-machine communication system for e-healthcare society*, Computers in Human Behavior.
17. Señor, I.C., Fernández-Alemán, J.L. & Toval, A. (2012). Are personal health records safe? A review of free web-accessible personal health record privacy policies, *Journal of Medical Internet Research*, 14 (4).
18. Sweeney, L. (2002). K-anonymity: A model for protecting privacy, *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10 (05), pp. 557-570.

19. Tang, P.C., Ash, J.S., Bates, D.W., Overhage, J.M. & Sands, D.Z. (2006). Personal health records: Definitions, benefits, and strategies for overcoming barriers to adoption, *Journal of the American Medical Informatics Association*, 13 (2), pp. 121-126.
20. Wafa, T. (2010). How the lack of prescriptive technical granularity in HIPAA has compromised patient privacy, *North Illinois University Law Review*, 30 (3).
21. Wagstaff, A. & Culyer, A.J. (2012). Four decades of health economics through a bibliometric lens, *Journal of Health Economics*, 31 (2), pp. 406-439.
22. Wang, C., McLee, Y. & Kuo, J. (2011). Mapping the intellectual structure of digital divide, *International Journal of Social Science Humanity*, 1 (1), pp. 49-54.
23. White, H.D. & Griffith, B.C. (1981). Author cocitation: A literature measure of intellectual structure, *Journal of the American Society for Information Science*, 32 (3), pp. 163-171.