Review

Information Privacy and Pervasive Health: Frameworks at a Glance

NaseriBooriAbadi T.[1], Sheikhtaheri A.[2]*

[1]School of Medicine, Shahroud University of Medical Sciences, Shahroud, Iran
[2]Health Management and Economics Research Center, School of Health Management and Information Sciences, Iran University of Medical Sciences, Tehran, Islamic Republic of Iran

*Corresponding author: A. Sheikhtaheri
Health Management and Economics Research Center, School of Health Management and Information Sciences, Iran University of Medical Sciences, Tehran, Islamic Republic of Iran
E-mail: sheikhtaheri.a@iums.ac.ir

Received: 26 June 2015
Accepted: 26 November 2015

ABSTRACT

Background: Health information is highly sensitive to all kinds of health care environments ranging from organization-based to personalized health. Nowadays, health information is exchanged readily for the consequence of the introduction of ubiquitous computing in healthcare industry. Therefore, minimization of vulnerabilities and security risks are a must. Information privacy is a critical issue in all kinds of health information systems with some platforms (e.g. implementable medical devices, mobile-based apps, biosensors, smart home, etc.).

Objective: This paper was aimed at providing a snapshot of existing frameworks protecting health information privacy in pervasive health care environments.

Methods: Accordingly, terms such as “pervasive health care”, “mobile health”, “ubiquitous health”, “health information” and “privacy” were searched in technical databases and on the Internet search engines using free text both in English and Persian (February 2015).

Results: In summary, these frameworks have characteristics as managing data access, data collection, use and disclosure in common.

Conclusion: Taken together, these frameworks would be applied in emerging health environments and associated frameworks addressing information privacy.

Keywords

Privacy, Security, Pervasive Healthcare

Introduction

Over the years, health care delivery model has been transformed several times. For instance, 200 years ago, health care was provided to patients through a family physician in their homes. Since the 20th century, health care services have been centralized in hospitals, and it gradually shifts towards near-the-patients location in the advent of emerging technologies, including wireless communication and mobile devices [1, 2]. In fact, information and communication technology (ICT) are transforming the face of health care delivery from organization-based to personalized one [3] facilitating patients’ status monitoring ubiquitously in a non-invasive way [4].

In parallel with these trends, medical records have been subject to great changes according to its 4000-year history, ranging from papyrus text (in 1600 B.C.) physicians narrative records of hospital structured forms (at the end of the 19th century), afterwards, to different forms of electronic health records (at the end of 21st century) [5].

Nowadays, an increasing prevalence of many chronic health conditions is the prime cause of death all over the world [6]. Furthermore, according to studies, the burden of chronic health conditions has risen among all individuals in many countries, especially developing nations [7]. Moreover, health care costs are escalating as growing elder population [8] as the elderly are more vulnerable to diseases particularly chronic conditions [9, 10]. In addition, healthcare is changing because of the shifting of telemedicine from desktop platforms to wireless and mobile configuration as society has become mobile [11]. Therefore, pervasive health care (e.g. smart home, mobile and ubiquitous telemedicine, pervasive patient monitoring, intelligent emergency monitoring and pervasive life style management) is widespread across the world, aiming at economizing health care resources, providing health care efficiently as well as managing chronic conditions [12، 13].

On the whole, technology advancement intensified individual and organizational privacy concerns for common characteristics, including ubiquity, invisibility, sensing and memory augmentation [14]. Obviously, studies have shown the risks as data modification, impersonation, eavesdropping, and replaying may endanger health information security and privacy [15]. According to National Committee for Vital and Health Statistics, health information privacy is defined as "the right to control the acquisition, uses or disclosures of individually identifiable health information" [16]. In recent years, researchers examined important issues, especially privacy issues in pervasive healthcare despite the fact that it is an evolving concept [17]. Literature revealed that several frameworks in this regard developed over the years. This paper was aimed at providing a snapshot of such a framework protecting health information privacy in pervasive healthcare settings to obtain an outlook for developing a customized overarching framework in terms of common concepts as well as exclusive ones.

Methods

This review study was conducted searching following terms such as "pervasive health care", "mobile health", "ubiquitous health", "health information", "framework" and "privacy" in PubMed-Medline, Springer, Magiran, Scientific Information Databases and on the Internet search engines using the free text both in English and Persian in February 2015. Relevant frameworks were retrieved and compared.

Results

Here, some major frameworks are outlined comprising actionable principles protecting health information privacy (Table 1).

These frameworks look alike in the light of major themes, displayed as the core of our proposed framework in Figure 1. It does not make any difference which health information has been exchanged in conventional or modern health care settings, considering these common issues is imperative. Depending on the context of the subjected framework being used some technical items, for instance, particular items both in m-Health and Implantable Medical Devices (e.g. adaptability, availability, manageability and privacy and security issues related to IMDs) would be added.

Reviewing aforesaid frameworks indicated that privacy protection frameworks developed based on previous ones, over the years and developed gradually. In parallel with the emergence of new technologies, new issues and challenges are detected, and researchers seek appropriate solutions meeting the requirements of privacy improvement and its reinforcement.

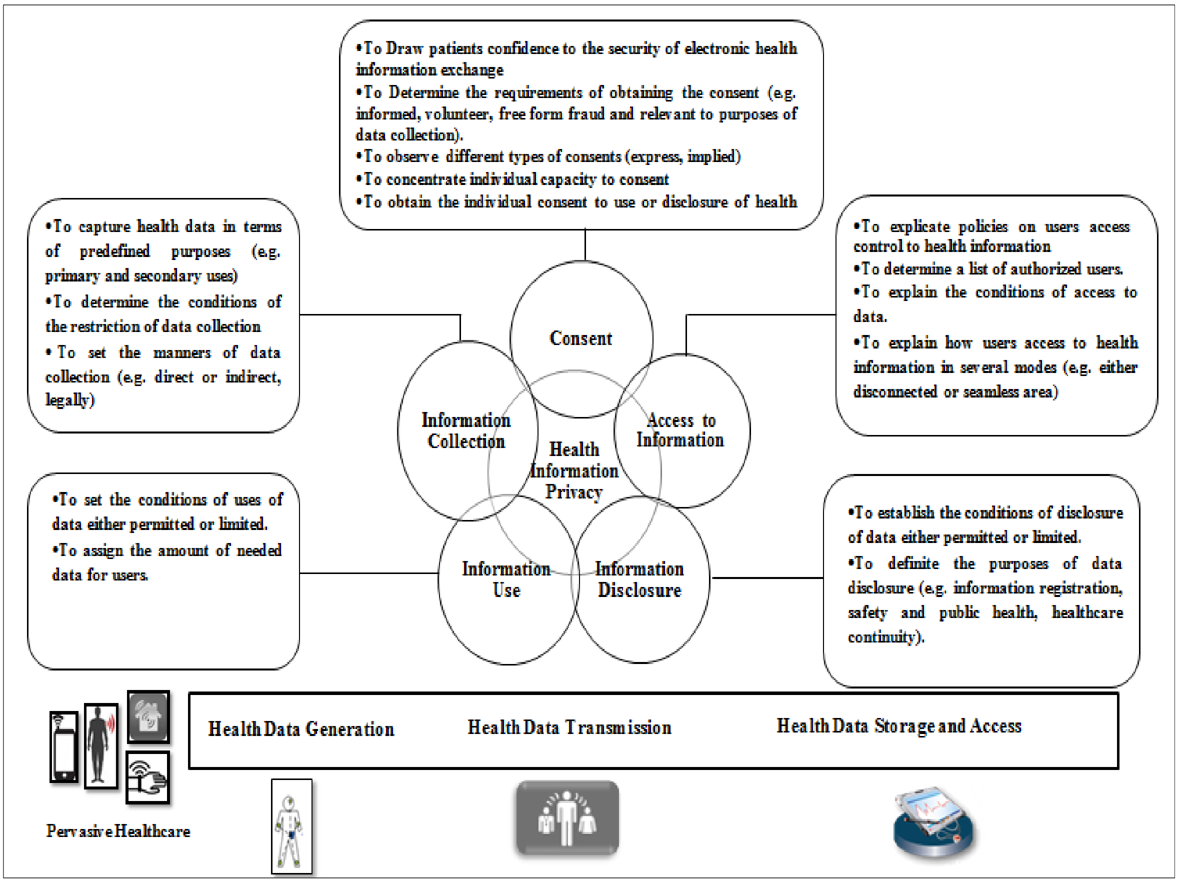
Discussion and Conclusion

The potential risks to individuals' informa-

Table 1: Frameworks for the Protection of Health Information in a Pervasive Health Environment.

Framework	Objective	Components
Markle Common Framework for Networked Personal Health Information [18, 19]	To indicate the way of health information exchange and protection.	Fair Information Practice Principles were the core of this framework. It contains 16 policies and technical documents; model contract language.
National Framework for Electronic Exchange of individually identifiable health information [20]	To guide public and private entities in order to hold and exchange health information properly.	The international, national, and public and private sector privacy and security principles, concentrating on individual information in an electronic environment, particularly individually identifiable health information such as popular privacy frameworks (e.g. Asia-Pacific Economic Cooperation privacy framework), related guidelines (e.g. Organization for Economic Cooperation and Development (OECD) Guidelines on the protection of privacy and personal data exchange across the countries) relevant Acts (e.g. Personal Information Protection and Electronic Documents Act and Health Insurance Portability and Accountability Act)
Framework for health information on wearable devices [21]	To address major security requirements in wireless body area network	A comprehensive privacy protection package based on existing frameworks categorized in three groups, including data storage (e.g. confidentiality, ongoing control over and dependability); data access (e.g. access control/privacy, accountability, abrogation the violator's accessibility to data, and strictly tracking user activities) and also encompassing authentication and availability
Conceptual privacy framework for health information on wearable device [22]	To provide complete privacy protection package to wearable device owners.	Markle Common Framework for Networked Personal Health Information and The Certification Commission for Health IT Framework has formed this framework. It contains 10 principles and 9 checklists.
Framework Model and Principles for Trusted Information Sharing in Pervasive Health [23]	To analyze pervasive health care in terms of trustworthiness and privacy challenges.	This includes following concepts: Information space, pervasive health, trust, systems, stakeholders' interest/concerns, environment, and privacy
A general framework for evaluating the security and privacy of next-generation wireless implantable medical devices [24]	To recognize the design goal of security and privacy for implantable medical devices.	It consists of some criteria for implantable medical devices including, safety and utility as well as security and privacy.
A Privacy framework for mobile health and home-care systems [16]	To restate common framework principles and describe privacy properties being used in health systems.	Common framework, health privacy best practices; The Certification Commission for Health IT Framework and ONC principles have built it. Moreover, many special items unique to m-Health (e.g. adaptability, the possibility to growing use, efficiency, usability, manageability, and availability.

tion privacy are associated with the disclosure of personal health information either deliberately or unintentionally both in conventional and pervasive health care settings. However, in comparison with conventional health care delivery, pervasive health care, a dynamic and open culture of information sharing among all health care stakeholders entails more concentration on privacy issues. The more readily and quickly health information exchange



•To Draw patients confidence to the security of electronic health information exchange
•To Determine the requirements of obtaining the consent (e.g. informed, volunteer, free form fraud and relevant to purposes of data collection).
•To observe different types of consents (express, implied)
•To concentrate individual capacity to consent
•To obtain the individual consent to use or disclosure of health

•To capture health data in terms of predefined purposes (e.g. primary and secondary uses)
•To determine the conditions of the restriction of data collection
• To set the manners of data collection (e.g. direct or indirect, legally)

•To explicate policies on users access control to health information
•To determine a list of authorized users.
•To explain the conditions of access to data.
•To explain how users access to health information in several modes (e.g. either disconnected or seamless area)

•To set the conditions of uses of data either permitted or limited.
•To assign the amount of needed data for users.

•To establish the conditions of disclosure of data either permitted or limited.
•To definite the purposes of data disclosure (e.g. information registration, safety and public health, healthcare continuity).

Figure 1: Proposed Framework on Protection of Health Information Privacy in Pervasive healthcare.

among different entities (e.g. health care organizations, health care providers, and payers as well as patients), the more the risk of privacy breach.

Given the above discussion, information privacy is a critical part of the right to privacy. Therefore, considering the incontrovertible effect of ICT in processing medical information, protecting information privacy is the prime challenge faced by health information custodians especially in modern personalized health care systems. Taking a look at popular frameworks, it seems that most of them have common characteristics in the protection of personal health information. These are embedded at the center of this proposed framework (Fig. 1), articulating five main areas, including health information collection, the obtainment of individual consent prior to authorized users access, disclosure and use of health information in a pervasive healthcare setting (e.g. m-Health, Implantable Medical Devices, monitoring individual health status from distance). As a whole, the principles of privacy protection of health information are considered in a continuum ranging from health data generation, transmission to storage and access.

The right understanding of common Information and Communication Technologies (ICTs) and monitoring the emerging technologies seems imperative in the development of privacy protection of health information. However, this framework is based on information collection, use, disclosure and the right of individuals to access to personal health information (both manual and electronic), consideration of modern and different platforms leading to recognizing the potential drawbacks.

Entirely, "privacy" concept evolves over the years. The advent of new technologies is influential in this regard. Normally, it appears that this new concept requires more attention to get mature. Therefore, making more efforts for others to learn from their best practices, applied guidelines, existing frameworks in view of the national high rate of penetration of modern technologies (e.g. telemedicine, teleconsultation and telecare) and public adoption of ICTs (e.g. personal computers, tablets, mobile phones, smart phones and social networking sites) deems necessary.

In summary, some relevant conceptual and practical frameworks are described in brief. These frameworks were similar in basic principles governing data access, collection, use, and disclosure. In conclusion, it is wise to consider the common concepts as building blocks of forthcoming frameworks on the protection of privacy in the emerging health environment.

Conflict of Interest

None

References

1. Arnrich B, Mayora O, Bardram J, Troster G. Pervasive healthcare: paving the way for a pervasive, user-centered and preventive healthcare model. Methods Inf Med. 2010;49:67-73. doi: 10.3414/ME09-02-0044. PubMed PMID: 20011810.
2. Das R. A paradigm shift in healthcare: changing business models and the impact of technology. Global Healthcare. 2009.
3. Blobel B. Architectural approach to eHealth for enabling paradigm changes in health. Methods Inf Med. 2010;49:123-34. doi: 10.3414/ME9308. PubMed PMID: 20135083.
4. Custodio V, Herrera FJ, Lopez G, Moreno JI. A review on architectures and communications technologies for wearable health-monitoring systems. Sensors (Basel). 2012;12:13907-46. doi: 10.3390/s121013907. PubMed PMID: 23202028; PubMed Central PMCID: PMC3545599.
5. Gillum RF. From papyrus to the electronic tablet: a brief history of the clinical medical record with lessons for the digital age. Am J Med. 2013;126:853-7. doi: 10.1016/j.amjmed.2013.03.024. PubMed PMID: 24054954.
6. Rafii F, Fatemi NS, Danielson E, Johansson CM, Modanloo M. Compliance to treatment in patients with chronic illness: A concept exploration. Iran J Nurs Midwifery Res. 2014;19:159-67. PubMed PMID: 24834085; PubMed Central PMCID: PMC4020025.
7. BAGHERI LN, AZIN A, SADIGHI J, JAHANGIRI K, AEENPARAST A, OMIDVARI S, et al. Chronic diseases in a population-based study: Iranian Health Perception Survey (IHPS). 2011.10:391-5
8. Mann WC, Helal S, editors. Pervasive computing research on aging, disability and independence. Applications and the Internet Workshops, 2004 SAINT 2004 Workshops 2004 International Symposium on; 2004: IEEE.
9. Darabi S, Torkashvand M, Latifi G. Socioeconomic outcomes of Iranian elderly population 1951-2051. Journal of Monthly Book of Social Sciences 2013;58:17-28.
10. Denton FT, Spencer BG. Chronic health conditions: changing prevalence in an aging population and some implications for the delivery of health care services. Can J Aging. 2010;29:11-21. doi: 10.1017/S0714980809990390. PubMed PMID: 20202262.
11. Vouyioukas D, Maglogiannis I. Pervasive and smart technologies for healthcare: ubiquitous methodologies and tools. Pervasive and Smart Technologies for Healthcare: Ubiquitous Methodologies and Tools IGI Global. 2010:984-1014.
12. Sneha S, Varshney U. Enabling ubiquitous patient monitoring: Model, decision protocols, opportunities and challenges. Decision Support Systems. 2009;46:606-19. doi: 10.1016/j.dss.2008.11.014.
13. Wickramasinghe N. Pervasive computing and healthcare. Pervasive Health Knowledge Management. 2013:7-13. doi: 10.1007/978-1-4614-4514-2_2.
14. Jafari S, Mtenzi F, O'Driscoll C, Fitzpatrick R, O'Shea B. Measuring privacy in ubiquitous computing applications. Int J Digit Soc. 2011;2:547-50.
15. Al Ameen M, Liu J, Kwak K. Security and privacy issues in wireless sensor networks for healthcare applications. J Med Syst. 2012;36:93-101. doi: 10.1007/s10916-010-9449-4. PubMed PMID: 20703745; PubMed Central PMCID: PMC3279645.
16. Kotz D, Avancha S, Baxi A, editors. A privacy framework for mobile health and home-care systems. November 13 - 13, 2009. New York: Proceedings of the first ACM workshop on Security and privacy in medical and home-care systems; 2009: ACM .
17. Madeira RN, Postolache O, Correia N, Silva O. Designing a pervasive healthcare assistive environ-

ment for the elderly. Ubicomp 2010. 2010. doi: 10.1.1.474.9169.

18. Health Information and Management Systems Society. Managing Information Privacy & Security in Healthcare: Markle Common Framework for Privacy and Secure Health Information Exchange. Health Information and Management Systems Society. 2013.
19. McGraw D. Comprehensive Privacy and Security: Critical for Health Information Technology. White paper. 2008.
20. Health UDo, Services H. The nationwide privacy and security framework for electronic exchange of individually identifiable health information. Office of the National Coordinator for Health Information Technology. 2008.
21. Li M, Lou W, Ren K. Data security and privacy in wireless body area networks. IEEE Wireless communications. 2010;17:51-8. doi: 10.1109/MWC.2010.5416350.
22. Safavi S, Shukur Z. Conceptual privacy framework for health information on wearable device. PLoS One. 2014;9:e114306. doi: 10.1371/journal.pone.0114306. PubMed PMID: 25478915; PubMed Central PMCID: PMC4257553.
23. Ruotsalainen P, Blobel B, Nykanen P, Seppala A, Sorvari H. Framework model and principles for trusted information sharing in pervasive health. Stud Health Technol Inform. 2011;169:497-501. PubMed PMID: 21893799.
24. Halperin D, Heydt-Benjamin TS, Fu K, Kohno T, Maisel WH. Security and privacy for implantable medical devices. IEEE Pervasive Computing. 2008;7:30-9.