Jurnal Integrasi
Vol. 8, No. 2, October 2016, 111-114
p-ISSN: 2085-3858

Article History
Received August, 2016
Accepted September, 2016

The standardization of Electronic Health Record system in used in cross-organizational platform

Ade Syahputra*, Budi Arifitama*

* Universitas Trilogi
Program Studi Teknik Informatika
Jl. Kampus Trilogi/STEKPI no.1, Kalibata, Jakarta 12760, Indonesia
E-mail: adesyahputra@universitas-trilogi.ac.id
E-mail: budiarif@universitas-trilogi.ac.id

Abstrak

Perkembangan Teknologi Informasi saat ini memiliki pengaruh yang signifikan terhadap pertumbuhan e-Health. e-Health merubah model pelayanan kesehatan dan penyampaian informasi kepada masyarakat melalui penggunaan Internet. e-Health diperkenalkan sebagai solusi yang menjanjikan efektivitas biaya dan kualitas pelayanan kesehatan. Dengan menggunakan e-Health, pasien dapat dengan mudah berkonsultasi dengan profesional kesehatan, mendapatkan informasi yang berkaitan dengan penyakit tertentu, dan mengakses catatan medis. Penulisan ini akan membahas tentang salah satu masalah yang terdapat pada e-Health terkait dengan catatan medis pasien yang dikenal sebagai Electronic Health Record (EHR). EHR digunakan untuk mendokumentasikan informasi kesehatan pasien dalam format digital. Kualitas informasi yang terdapat pada EHR sangat penting bagi tenaga kesehatan untuk mengambil keputusan dalam perawatan pasien. Masalah yang muncul dan menjadi kontemporer adalah terdapat pada standarisasi sistem EHR. Pembahasan dalam penulisan ini akan fokus pada standarisasi sistem EHR terkait dengan penggunaan data di lintas organisasi termasuk *data sharing*, keamanan data dan *data preservation*.

Kata kunci: Internet, e-Health, Healthcare

Abstract

The development of Information Technology has a significant influence to the growth of e-Health these days. e-Health changes the model of health services and information delivery to the people through the use of Internet. e-Health has been introduced as a solution that promises cost effectiveness and quality of services in healthcare. Using e-Health, people can easily consult with health professionals, get information related to the specific diseases, and access their medical records. This paper will discuss about one of the current issues in e-Health which is related to the patient medical records known as Electronic Health Record (EHR). EHR is used primarily for documenting patient health information in digital format. The quality of information which contains in EHR is extremely important for health expertise in making decision for patient care. The issue that appear and being contemporary is on the standardization of EHR system. The discussion in this paper will more focus on the standardization of EHR system which is related to the use of the data in cross-organizational platform includes data sharing, data security and data preservation.

Keywords: *Internet, e-Health, Healthcare*

1 Introduction

E-Health has been introduced and changes the model of health services and information delivery through the use of Internet technology. The initiative use of Internet technology enables healthcare institutions to organize their activities and provides cares in ways that were impossible before. The patients can actively participate in setting objectives and planning their own care with assist from healthcare expertises. Thus, e-Health becomes a promise solution for such problems within healthcare services such as high cost of delivery, medical errors, lack of access, and lack of communication between healthcare expertises and patients.

One of the current issue in e-Health is related to the electronic record of patient health information which known as Electronic Health Record (EHR). Since the

increasing number of healthcare institutions that used EHR system, this causes widely open the opportunities for shared care between different institutions. The issue that appear and being contemporary is on the standardization of EHR system. This is because different healthcare institutions usually use different internal scheme. Therefore, the needs for implementing the standard of EHR system is significantly important in order to enable the sharing of patient health information with the support of a secure system and good data preservation. Thus, this paper will discuss about the standardization of EHR system in used in cross-organizational platform which more focus on the discussion about data sharing, data security and data protection, and data preservation.

2 Literature Review

Hesse and Shneiderman (2008) find that as the healthcare technology advances and health information environment has grown more complex, healthcare becomes more susceptible to error. The analysis from medical charts of women with late state cervical cancer shown that due to the lack of mechanism in the medical system, the number of the deaths are increased. This situation should not happen if the health technology supports the standard healthcare mechanism. Moreover, allowing the patient to get involve in manage their own healthcare could have effects on increasing the patient's awareness in health and reduce the number of deaths.

E-Health has been introduced as the new model of health services that promises cost effectiveness and quality of services through the use of the Internet. The use of Internet technology enables the effectiveness communication between patients and healthcare expertise which contribute to patient education and improved healthcare outcomes [11]. E-Health also enables the different institutions to exchange or share the patient health information (EHR). Thus, the change in the form of health services and information delivery brings new challenges to the standard of care.

In relation with EHR system, lot of healthcare institutions used the different structure of the system [8]. This affects to the communication and exchange the information cross-organizational platform. Some issues that appear are related to the security, protection, and preservation of patient's data. Thus, the standardization of EHR system is considerably important to be develop in order to enable the sharing of patient health information with the support of a secure system and good data preservation.

3 Discussion

a. Data Sharing

The increasing numbers of healthcare institutions that using e-Health system causes widely open the opportunities for closely co-operate between institutions. In relation with Electronic Health Record (EHR), healthcare institutions share the patient health information in order to offer a high quality of patient care. However, the main issue in sharing EHR between different institutions is on the standardization of a secure and trust communication cross-platform. According to Van der Haak et al. (2003), secure and trust communication cross-platform is significantly important to be developed. This platform is needed to be developed in order to ensuring the flow of communication is secure and makes it possible to share sensitive information between different platforms and across borders of e-Health services.

Ruotsalainen (2004) stated that it is difficult for different healthcare institutions to trust each other regarding the sharing of sensitive data. The healthcare institutions need a mechanism that could built trust between different institutions and also have to meet the security requirements. The security requirements are another issue that should be address because different healthcare institutions usually use different internal security scheme. Ruotsalainen (2004) suggests the institutions need to implement the cross-platform model that use existing commercial security bridging services for connected domains from different organizations. Moreover, the platform should also support both data transfer and data access communication models in order to enable the communication.

Blobel (2001) gives the example of a model that provides a secure inter-organizational communication and information sharing. The name of the model is HARP which funded by the European Commission within the Information Society (IST) programme. The objective of HARP model is strengthening the distributed, component based, secure applications in client server environments on Internet technology. HARP Cross-Security Platform (HCSP) has been applied in this model to enable the communication in different environment. HARP also provides 'an initial degree of automation in building secure medical Internet-based applications' [2]. The current version of HARP has been developed using UML and Rational Rose Methodology. Thus, HARP would be possible to adopt other open specification such as CORBA in order to provide the trustworthy way of communication and co-operation in different environment.

Another example of a secure and trust communication cross-platform is evolutionary model which proposed by Ruotsalainen (2004). This model is using the

combination of national security domain and regional with the help of Internet portal. Basic security services, such as security policy bridging, cross-domain identification and authentication, certification services, static privilege management, and auditing services, are used in order to centrally manage the cross-organizational communication. The benefits of this model are 'the platform requires minimal changes to present legacy systems, it integrates present regional and national networks, and acts as a migration path to future, purely internet-based health information systems' [10].

As can be seen from previous examples, these two models are concerned with providing the platform which addresses the needs of secure and trustworthy way in communication and co-operation in different organization. The secure and trust communication cross-platform is highly important because this platform is used to sharing sensitive data, such as EHR, which is mainly important in providing a continuity and integrity of treatment processes to the patient. Thus developing this platform will have direct effects on the quality of patient care.

b. Data security and data protection

The use of internet as a media in access and sharing Electronic Health Record (EHR) is associated with some risks. The kinds of risks such as manipulate, steal, damage or destroy information are enormously danger to the patient care and patient information security [14]. Yee (2007) stated that it is highly important to take actions for protecting patient information by analysing and identifying "where" and "what" kind of protections that are needed to be taken. Therefore, the aspects of data security and data protection are needed to be highly concerned to prevent the threats to patient information.

There are some technical solutions that can be use in order to provide security and protection to patient information. One of the related applications is Cryptography algorithm. Encryption is used to changed or encode the data in such way where only authorized people can read the content by change the data back to its original form [5]. There are two forms of cryptography algorithms namely symmetric and asymmetric algorithm. These two algorithms could guarantee data security and data protection of confidential patient information. However, Van Der Haak et al. (2003) stated that even these algorithms could give a good protection and security, the combination of these algorithms is often used in real world to obtain a high security of data.

Another type of application that can be implemented in healthcare institutions is The Patient-Centred Access to Secure Systems Online (PCASSO). PCASSO was developed to enable healthcare expertise and patient to save access to patient health information over the Internet [4]. This application is using multiple security functions such as biometric devices, passwords, firewalls, and digital signatures. Due to the use of multiple security functions, Masys et al. (2002) find that PCASSO has high ratings in terms of security. However, Smith and Eloff (1999) points out the protection that provide by PCASSO illustrates the complexity of the application. The author suggested that this application need to adopt flexible and configurable functions besides providing securely access to patient's data.

From these two examples, it can be seen that the aim of data security and data protection is to ensure confidentiality, integrity, authentication, accountability and availability in using, storing and exchanging the patient's data (EHR) [9]. Early detection on the threats will prevent EHR, which contains information of the utmost sensitivity, from under control of unauthorized person or party.

c. Data preservation

Electronic Health Record (EHR) contains of the documentation of patient health information which is stored in digital format. Growing, dynamic and critical data of patient that recorded in EHR is the main problem in data preservation. Scott (2007) believes the issues that appear related to the information content are technological change, the ravages of time and decaying media. These issues have significant impact to data preservation including storage options, storage media, technology obsolescence, cost and scale. Furthermore, in relation with the issues, Blažiča et al. (2007) points out that it needs a stable framework that could ensure long-term data preservation which will prevent from the risk of losing data.

In the paper, Scott (2007) provides a variety of potential solutions including strategy and policy which required ensuring long-term access use of information. The kinds of solutions, such as data migration, extensibility, data refreshing, emulation, data filtering, and backward compatibility, are proposed in order to ensure the data remain accessible with no loss of the integrity of information. However, these solutions or strategies that are provided by the author are not internationally accepted. Scott (2007) also mentioned that healthcare institutions need to take an initiative to implement patient health record with integrated data preservation strategies that ensure availability and integrity of information content.

In the same way, Moore (2006) suggests the generic software called Data grid as a potential solution for data preservation. Data grid is a technology that provide data management infrastructure which can be used to implement records preservation environments. This software has 'the ability to interact with multiple

types of storage systems, automating the processes of preservation, reducing risk of data loss through reproduction of digital component, ensuring the permanent association of identity and integrity metadata with records, and supporting retrieval and access' [13]. With these capabilities, data grid technology could address the issue of technology evolution to protect the records from accidental change and ensuring that preservation environments can take advantage of more cost-effective technology.

As can be seen, limited research has been conducted by some researchers which show that data preservation is a critical issue. Further work is required to understand the appropriate formats, standards or solutions that could internationally accepted and implemented regarding data preservation. Moreover, a stable framework of data preservation is important to be applied internationally with using future technology advances that could safe guarding the data and capable to be accessed in real time.

6 Conclusions

It is essential for healthcare institutions that providing e-Health services to have a standard Electronic Health Record (EHR) system. This will give the benefits for the institutions to bridging the communication and sharing the data cross-organizational platform. Futher research is needed to have an international/national standard of EHR system that offers a secure system and good data preservation. Thus, EHR as part of e-Health as a new model of health services could provide a high quality of patient care that promises cost effectiveness to the patient.

References

[1] A.J. Blažica, T. Klobucarb, and B.D. Jerman, , "Long-term trusted preservation service using service interaction protocol and evidence records", *Computer Standards & Interfaces*, **29**, pp.398-412, 2007.

[2] B. Blobel, , "Trustworthiness in distributed electronic health care records – basis for shared care", *CSDL.Computer.org*, pp.1-9, 2001.

[3] B.W. Hesse, and B. Shneiderman, "eHealth research from the user's perspective", *BIH Public Access*, **32**, pp.97-103. 2008.

[4] D. Masys, D. Baker, A. Butron, and K.E. Cowles, "Giving patients access to their medical records via the internet", *Journal of the American Medical Informatics Association*, **9**, pp.181-191, 2002.

[5] E. Smith, and J.H.P. Eloff, "Security in health-care information systems – current trends", *International Journal of Medical Informatics*, **54**, pp.39-54, 1999.

[6] G.. Yee, "Visual analysis of privacy risks in Web Services", *IEEE Computer Society*, pp.671-678, 2007.

[7] K. Häyrinena, K. Sarantoa, and P. Nykänenb, "Definition, structure, content, use and impacts of electronic health records: A review of the research literature", *International Journal of Medical Informatics*, **77**, pp.291- 304, 2007.

[8] K. Smith, and D.Kalra, "Electronic health records in complementary and alternative medicine", *International Journal of Medical Informatics*, **77**, pp.576-588, 2008.

[9] M. Van der Haak, A.C. Wolffa, R. Brandnera, P. Dringsb, M. Wannenmacherc, and Th. Wettera, "Data security and protection in cross-institutional electronic patient records", *International Journal of Medical Informatics*, **70**, pp.117-130, 2003.

[10] P. Ruotsalainen, "A cross-platform model for secure Electronic Health Record communication", *International Journal of Medical Informatics*, **73**, pp.291-295, 2004.

[11] R. Kukafka, J.S. Ancker, C. Chan, J. Chelico, S. Khan, S. Mortoti, K. Natarajan, K. Presley, and K. Stephens, "Redesigning electronic health record systems to support public health", *Journal of Biomedical Informatics*, **40**, pp.398-409, 2007.

[12] R.E. Scott, "e-Records in health—Preserving our future", *International Journal of Medical Informatics*, **76**, pp.427-431, 2007.

[13] R.W. Moore, "Building preservation environments with data grid technology", *The American Archivist*, **69**, pp.139-158, 2006.

[14] T.L. Wiant, "Information security policy's impact on reporting security incidents", *Computers & Security*, **24**, pp.448-459, 2005.