Review of e-Health Frameworks

Biraj Prajapati, Prof William J Buchanan, Richard Macfarlane, Adrian Smales, Greg Spyra
Edinburgh Napier University
10 Colinton Road, Edinburgh

In order to improve the quality of health care and widen the accessibility, health care providers are consistently looking to inject information and communication technology to the traditional health care system (Mair, et al., 2012). This process can be defined as e-health. World Health Organization (WHO) has defined E-Health as “the use of information and communications technologies (ICT) in support of health and health-related fields, including health-care, health surveillance, health literature, and health education, knowledge and research” (Blaya, et al., 2010). In other words, e-health can be defined as the use of information technology in order to make a progressive approach in the field of health care. This paper outlines some of the developments in the creation of e-Health framework, and which aim to create an integrate approach to e-Health. This includes the DACAR e-Health framework developed in collaboration between Imperial College, London and Edinburgh Napier University, and which was implemented within Chelsea and Westminster Hospital, London.

1. INTRODUCTION

The past decade has seen the constant growth on the study and research related to the implementation of e-health system and its evaluation. A study has found out that 56%-79% of internet users in US seek health information over the internet (Andreassen, et al., 2007). People from all around the world have started making a great use of technology for their healthcare system. Thus, the national health authorities around the world such as English NHS, German Telematic platform, danish sundhed.dk etc. have began to focus on different e-health services such as electronic patient record, electronic health cards and electronic health portals (Andreassen, et al., 2007). Many innovative forms of electronic health care services have been evaluated over the past few years in order to analyse benefits, costs and potential consequences through it. There are also some certain requirements that an efficient and trustworthy e-health system should possess.

2. E-HEALTH SYSTEM REQUIREMENTS

Many surveys have been carried out around the world in relation to the requirements for use of technologies in the medical field and it was found out that security and privacy are the two most important requirements. Thus, it plays a vital role in successful implementation of e-health and other medical technologies. A survey found out that females and healthy adults require more security and privacy standards in comparison to the males and ailing elderly (Wilkowska & Zießle, 2012). The sensitive data stored in an e-health system implies that an e-health system should always have proper security and privacy policy because the disclosure of any of the patient’s data could have a severe consequences. The leakage or the disclosure of the data may also result in legal penalties to the health system providers for violating the privacy laws.

Eysenbach (2001), in his paper, has put together 10 e’s that characterizes an e-health. These 10 e’s can also be classed as a requirement for the e-health system. According to Eysenbach (2001), an e-health should be efficient, evidence based and equitable. It should enhance the quality of care and also follow the patient-physician ethics. It should prioritise the education of health care workers via online sources and also enable the exchange of information in a uniform method. Finally, an e-health should also encourage relationship between patients and health professionals, resulting in the extension of scope of health care beyond the conventional boundaries (Eysenbach, 2001).

Although patient centric e-health system is the future for e-health system, there are lots of challenges that need overcoming if it is to be successfully implemented over the coming years (Ball & Lillis, 2001). It's not just the technical challenges that needs overcoming, but also the support and awareness for the patients, which would include consumer education, physician/ consumer communication, administrative efficiencies, clinical decision support and disease management (Ball & Lillis, 2001).

Along with all these requirements, it is also necessary that an e-health system complies with
laws related to the medical data sharing in a country. This would include the data protection act or a similar ethical act.

Availability of e-health services all the time has also been cited as one of the major requirements of an e-health system by AbuKhousa, et al. (2012). In an emergency situation, the loss or an unavailability of e-health system could result in severe consequences in patient’s life, thus, it is necessary that the e-health system is available all the time (AbuKhousa, et al., 2012).

3. CURRENT STATE OF E-HEALTH

The injection of IT in the field of health care has become progressively important to many countries around the world in recent years. e-health has many advantages in terms of cost efficiency and improvement of personal health management. Thus, there has been a continuing global effort aiming to implement some form of e-health system.

Hsu, et al. (2005) carried out a longitudinal and population-based evaluation on the use of e-Health service in Northern California state of USA between 1999 and 2002, where over 3 million people utilised the e-health services provided by Kaiser Permanente-Northern California (KPNC), an integrated delivery system for e-health services. Their study involved e-health service members who used a web-based secure portal to request the appointments with their doctors and order the prescription drugs.

In order to utilize the service provided by KPNC, patients were required to register in this service by requesting a password protected account through the website. When that request was received, the IDS delivered a mail that had a randomly generated pin to the member’s home address, who then could finalise the register using the pin and create a new personal password. This e-health system was mainly designed in order to facilitate the health records to the health worker and the patients had no access to their health records at all. Although this model found out that there was an increase in the number of users by more than 8% in the span of 3 years time, this model was only limited to the interest of health workers and the patients had a minimal role in it (Hsu, et al., 2005). Thus it was concluded that a lot of research was required in order to safely implement the e-health care system for the general public.

Canadian government began a plan to implement national e-health system in 2001, however, after 10 years when a qualitative study was performed on the progress, it was lagging behind many European countries in terms of implementation of national e-health care system, despite spending $1.6 billion. Lack of e-health policy was cited as one of the major reasons behind the failure of this plan, along with some of the approaches (Top-down) towards its implementation (Rozenblum, et al., 2011). Thus it was concluded that bottom-up, regional first approach was required for a successful implementation of an e-health technology.

Countries such as, Austria, Germany (German e-health card), and Taiwan (Taiwan electronic medical record template) are conducting many different works in relation to authentication and access control for e-health. In case of German e-health card, every citizens are provided with the smart card which contains the general administrative information. The same card could be used in order to access the medical information. Every smartcard consists of cryptographic keys and functions in order to identify each patient uniquely. Taiwan electronic medical record contains a similar infrastructure which are based on smartcards, however, this model of Taiwan is more concentrated on easy information sharing (Lohr, et al., 2010).

Similarly, NHS Scotland currently has its own e-health programme (2014-2020) that mainly aims to inject information and related technology with the intention of improving quality of patient care. The major strategic aims of this e-health programme includes supporting citizens to communicate and interact with NHS, manage their own health records, and improve the availability of the required information and tools for health workers in order to improve the quality of healthcare service. This programme also aims to facilitate everyone with digitally enabled information sharing solution, so that all the citizens and healthcare workers would be able to quickly access the information and required services, share the important information appropriately with the appropriate people and have an understanding on the information that is being shared, along with the confidence in its integrity, security and quality. Apart from accessing, sharing and controlling the information, it was also pointed out an e-health care system should be able to create an alert to trigger the people who are at risk. This programme is basically themed around placing people at the centre of health care and building partnerships between many health care bodies at local, regional and national level (Government, 2015).

At the current period though, health care systems of most developed countries face an uphill task to bring the improvement in the quality, efficiency, security and safety of the citizens’ medical data.

4. E-HEALTH FRAMEWORKS

Security and privacy of patients’ medical and personal information is a major concern in healthcare domains and there is a great need of extensive work in regards to the privacy and secure access to the patients’ records. There have been
many works carried out in the past in relation to the patients’ data security and privacy in an e-health system.

Sharing of the data is an important aspect in a e-health system. In an ideal e-health system, selected doctors or health care workers should be able to access patients’ data with the permission of patient. Russello, et al. (2008), in their paper, have suggested a workflow-based access control framework. In their framework, they have used the notion of workflow in order to capture the task one has to perform as the part of their duty, which would help to determine the required privilege. The model proposed by them is mostly based on the principle of granting least privilege in order to carry out their job (Russello, et al., 2008). In other words, an entity can have access to the resource for a certain length of time, only to perform their job, and once the work is completed, the access would be revoked. This model mainly follows the concept of role based access control for the health care system, and the decisions being made on the basis of the job performed by the entity. Even though Role base access control is considered as a state of art of the access control mechanism, this method is not flexible enough in order to cope with the demand that a health system or an e-health application presents in the current time.

Riedl, et al. (2008), in their paper, have introduced pseudonymization of information for privacy in e-health (PIPE) architecture in order to integrate primary and secondary usage of health data in an e-health system. Pseudonymization is a procedure in which a specifier replaces an identification data after being transformed into a specifier. This architecture provides an advanced concept for authorization, data sharing and data recovery, which would allow the restoration of access to the medical records even when the patient’s security token is lost. (Riedl, et al., 2008) claim that this concept could be used as a foundation for the national electronic health record initiatives or even as an extension to any existent e-health applications. It is also claimed that in this system, patients are totally in control of their data that has maximum security, which was achieved by the application of encryption method. The use of different encryption key in order to secure the database has also been proposed in this architecture, whereas the integrity of data is maintained by making the use of Transport Layer Security or making the use of hash values (Riedl, et al., 2008).

Ford, et al. (2009) proposes the Secure Anonymised Information Linkage (SAIL) Databank system in order to ensure the secure data transportation and reliable record matching method in order to facilitate precise linkage of data across the different medical datasets. This system accomplishes with the data protection act 1998 and makes the use of deterministic encryption of the data in order to anonymise and prevent the identification of individuals. This system also ensures that the data access is performed in a controlled environment and is properly authorised. Moreover, this system also addresses the data disclosure risk in data views (Ford, et al., 2009).

The use of Model-Driven application level encryption has been proposed by (Ding & Klein, 2010) in order to maintain privacy in the medical data. Their model is based on the application’s domain model, and generates the codes and configuration artifacts in order to control the encryption logic in the health system and modify database schema. The encryption is performed outside the database, thus, called application level encryption, which would allow flexibility in an e-health system. This model has also given special focus to the key management, giving special priority where the key is stored and who has the access to the keys. It is also argued in their paper that the use of randomly generated primary master key can be used in order to protect all the keys (Ding & Klein, 2010).

In order to provide the authentication and authorization for users to consume the services provided by e-health services, Han, et al. (2006) have proposed an authorization and authentication architecture for e-health services (A3AeHS) system that integrates both role based and attribute based method into the electronic health system. This model separates patients’ general data from the sensitive record and creates an authorization policy according to the sensitivity of the data. The authorization policy is also based on the role of the entity in the system, e.g. a GP has an access to all the records of patient whereas a social worker will have access to only certain data. This model is similar to the WBAC model (Russel, et al., 2008) discussed previously, however, the attribute based access control and the proposal of multi-factor authentication system in order to access the data has made this model superior over WBAC model.

Similarly, Fan, et al. (2011) have proposed Data Capture and Auto Identification Reference (DACAR) platform for e-health in cloud computing in order to overcome the concerns related to security, large scale deployment, service integration, large scale deployment, and integration and confidentiality of the medical data. DACAR platform includes Single point of contact (SPoC) to provide authentication and authorisation functionalities, rule based information sharing policy, and data buckets service in order to support the create, read, update and delete (CRUD) attribute which are hosted by cloud infrastructures. Some of the major issues that are addressed by DACAR are authentication, authorisation, data
Review of e-Health Frameworks
Biraj Prajapati ● Prof William J Buchanan

perspective, data integrity, data confidentiality and audit trail. Apart from all these, DACAR also include the functionalities for patient-centric e-health application, for eg: Early Warning Score(EWS) in order to react to any unusual data pattern (Fan, et al., 2011). DACAR platform also practices database-level encryption, using cryptographic signatures and kerberos authentication which ensures a great data security (Fan, et al., 2011).

Using DACAR platform, Ekonomou, et al. (2011), in their paper, have proposed a cloud based healthcare system which would integrate a formal health care system(DACAR) with an informal health care system (Microsoft Healthvault). This would enable the patients to share the health data on different health domain with their doctors, or someone who they prefer. They also claim that there is strong security and privacy of the medical data by following this practice, as the data security and privacy is ensured by both microsoft health vault and DACAR (Ekonomou, et al., 2011).

Similarly, Fengou, et al. (2013), in their paper, have proposed a framework that extends European Telecommunications Standards Institute (ETSI) architecture to deploy the standard services over next generation IP networks (Fengou, et al., 2013). The collaboration of European Telecommunications standards, 3rd Generation Partnership Project and parlay group have defined the joint working group in the context of open service access and is responsible for developing and maintaining open service access specifications. These specifications define accessing the network functionalities by making the use of application programming interface(API). Fengou, et al. (2013), propose the use of ETSI/Parlay specifications in their e-health domain. In their framework, they have defined profile classes to categorise the users:

- Patients profile
- Healthcare professional profile
- Aid person’s profile
- Operational domain’s profile
- Group profile

In terms of security in the framework, low-weight hash functions along with the combination of key is used in order to generate a message authentication codes(MACs), which is used to authenticate the users and prevent the unauthorized data disclosure in order to maintain the data integrity (Fengou, et al., 2013). Similarly, this model also uses “data integrity mechanism”, which was proposed by (Mantas, et al., 2009). In this method, data integrity is maintained by making the use of cryptographic smartcards, that contains secret keys, and MACs (Mantas, et al., 2009).

Lounis, et al. (2012) proposes a secure and scalable cloud-based architecture in order to deal with the challenges such as security and availability, created by the collection of health data with the means of medical sensor networks (Lounis, et al., 2012). They have claimed that the proposed mechanism for the data security is effective and flexible, as well as guarantees the confidentiality, integrity and access control to the medical data by making the use of combination of several cryptographic schemes. Their proposed framework considers two categories of users rather than five that was proposed by (Fengou, et al., 2013), i.e. patients and health professionals. Access control is achieved by making the use of attribute based encryption(ABE) in order to encrypt the data before storing it in database. There is a restriction to unauthorized access by using randomly generated symmetric key and security access policy which uses the combination of logical expressions through OR, AND or other operators. (Lounis, et al., 2012).

de Melo Silva, et al. (2014) have proposed the use of federated identity attributes for the secure storage and sharing of medical data in the cloud. They propose the use of SAML for the deployment of federated identity management. The collaborative networks between the institutions would enable the sharing of services between the users, and also enables the attribute management and facilitates single sign on. Like Lounis, et al. (2012), they too have proposed the use of attribute based encryption by providing users the cryptographic keys that would represent users true characters. They too, proposes the use of AND or OR operators and attributes to build a logical equation for security policies (de Melo Silva, et al., 2014).

The use of attribute based encryption is also supported by Li, et al. (2013), who proposes the use of individual secret key for every data owner(e.g. patient). It also supports the view of encryption of health record by using an encryption method, and implementation of role based access policy for users to access the data. They also claim that the security and access policy should be updated regularly, and there needs to be a provision of an audit trial to measure the effectiveness and security of data (Li, et al., 2013).

5. Conclusions

There are many e-Health frameworks proposed, each with key attributes, but there option requires a full review from experts, including those with a clinical and IT backgrounds. Without them, the sharing of information across disparate systems will be difficult, along with problems in sharing health entities in differing systems. The development of DACAR within Chelsea and Westminster Hospital provides one such model, and where the patient has full control of their own data, and where data can be moved from one hosting provider to
another. This work has since progressed to a spin-out company (Symphonic Trust).

6. Bibliography


Madsen, P. (Ed.). (2005, December 5). Liberty Alliance project (pp. 1-7). IEEE.