Confidentiality and Health: A Literature Review

Sulaiman Alateeq - Hari Hara Sudhan Viswanathan - Christobal Fuentealba - Haoran Pang –

Chenwei Hu - Sean Salisbury

Department of Computing & Information Systems

University of Melbourne

Abstract

Confidentiality in the growing Electronic Patient Records is a heated argument in the current world with heavy political involvement; this paper aims at learning how to achieve EPRs confidentiality through security policies to satisfy privacy legislations electronic health provisions. The literature part initially focuses on concepts involved in general and information security policies, and moves on towards the concepts of information security policy concepts, modules and mechanisms within the healthcare industry literature. The merits and demerits of these concepts will be discussed and an efficient model will be proposed in the discussion part. The paper discusses about finding efficient and effective approaches for formulating, implementing and refining security policies, and in enforcing them with appropriate procedures; and in analysing human behaviours to achieve the objective of achieving EPRs confidentiality. These information security policy modules and mechanisms includes of the Individual Identifiable Micro-data Technique, ETHICS method and Information Assurance policy compliance framework. The premise of this research also provide launch space with opportunities for future research.

Keywords: Health Security, Security Policy, EPR, Information Security, Confidentiality, Legislations, Patient Privacy, Electronic Record Share.

1. Introduction

Today's current advancements in technologies provide organizations great benefits such as enhancing their business processes and increasing their competitiveness. Similarly, organizations within the healthcare industry cannot resist the benefits of utilizing and adopting these technologies. Adopting these technologies includes digitizing patient health records to be Electronic Patient Records (EPR) (Angst & Agarwal 2009).

The use of EPRs includes the collection, storage, sharing and process of EPRs. EPRs provide many benefits for healthcare organizations such as seamless access, improved medical care, efficient sharing and cost effective information management (Rindfleisch 1997).

Despite the great benefits that EPRs deliver, the privacy of EPRs creates a problematic situation that rise the public's concern, in terms of preserving the confidentiality of an individual's health record (Anderson 2000). Since the introduction of EPRs, organisations have been able to collect massive amounts of patient data, which can be used to improve medical knowledge and general public safety. This data could also be used to highlight fraud and provide oversight, but invariably also leads to risks with confidentiality (Rodwin 2010). Especially those EPRs include highly sensitive personal information; and the disclosure of such information has significant negative implications such as social embarrassments, health insurance issues, difficulties in employment etc. (Angst & Agarwal 2009; Rindfleisch 1997).

Moreover, government legislations are formed to protect the privacy of an individual's health record. In 1996, the US government passed the Health Insurance Portability and Accountability Act (HIPPA) and subsequently released privacy rules in 2003 to strike a balance between protecting confidentiality and allowing legitimate use of health information (Wartenberg et al 2010). However, it is easy for lawmakers to lose sight that limiting access to this data could undermine the process of understanding and improving public health (Wartenberg et al 2010).

EPRs confidentiality concerns results in a difficult situation for healthcare providers, as it becomes difficult for them to provide quality healthcare, and can be in a position where they can jeopardise their professional image and suffer major consequences (Cannoy & Salam 2010).

Therefore, information security is a critical aspect in healthcare environments. Healthcare organisations must advancements in maintaining EPRs' confidentiality, and of all the tools available, the most widely used and valued is the information security policy (Stahl, Doherty & Shaw 2012).

This paper conducted a widespread literature review of information security policy and relevant healthcare security policy literature found within the healthcare industry, which includes different information security policy frameworks and techniques such as the Information Assurance framework, ETHICS, and the IIM techniques for achieving EPRs confidentiality. Discussion involved identifying the best-suited approaches for EPR's confidentiality, and merits and demerits were discussed. Based on the analysis, a mixture of ETHICS, IA Framework, and IIM can be a very suitable model in preserving the confidentiality of EPRs.

2. Literature Review

2. 1 Information Security

There are many definitions of Information Security out in the academia and in the industry, for the purpose of this paper Information Security is "the protection of information assets from accidental or malicious unauthorized disclosure, modification, or destruction, or the inability to process that information is necessary for a secure system" (Devargas 1995). This includes the protection of information from internal threats such as employee's computer abuse, and from external threats such as hacker's attacks (Rindfleisch 1997).

Accordingly, organisations need to understand the aspects behind information security management; and as identified by Wood (1997) these aspects include IT infrastructure, people, policies, standard, guidelines, procedures, and responsibility statements, all in which ensure efficient and effective information security management.

2.2 Information Security Policy

Policy is one of the critical factors in information security management context, and represents a powerful governance factor in the process of information security (Wood 1997).

Information security policy provides directions for organisations to define a framework of guidelines and to set the boundaries of its information security process. Furthermore, the support and commitment of senior management for information security policy assists in stating the rules that satisfy the vision of information security management (Höne and Eloff 2002).

2.3 As a Defence Measure

The primary role of the information security policy is to act as a deterrence tool by developing the staff's knowledge and awareness of information security, but alternatively it has been found to also coerce and threaten staff to comply with all of the policies (Stahl, Doherty & Shaw 2012).

2.4 The Information Security Policy Process

The process of information security policy involves the formulation, implementation, adoption and re-formulation of policies. This may require the creation of rules, procedures and guidelines or the evaluation and enhancement of current ones (Karyda, Kiountouzis & Kokolakis 2004). In addition, in order to ensure and further maximise the impact of information security policy, the human factor consisting of behaviour and attitude towards policy, must be addressed, to facilitate for information security policy compliance (Siponen Muhamood & Pahnila 2010).

2.5 Human Behaviour

Human behaviour is of a crucial importance to the success of information security policy, and is required to be influenced to facilitate policy compliance (Siponen, Muhamood and Pahnila (2010). Human behaviour can be approached by various means such as security training, education and awareness (SETA) programs, management support and commitment, compliance benefits and sanctions. Subsequently, employees' compliance for information security derives from employees' awareness and perception of existing policies of an organisation (Bulgurcu, Cavusoglu & Benbasat 2010). Furthermore, aspects such as the actual styling, wording, and presentation of security policies help encountering this human factor (Höne & Eloff 2002).

2.6 Information Security Policy Constructing Components

Karyda, Kiountouzis and Kokolakis (2004) proposed a contextual framework in figure 1, to help organisations to understand the dynamic nature of security policies and the various factors and activities that affect their formulation, implementation and adoption. Such understanding and awareness of the factors and activities facilitates developing suitable and effective security policies for organisations' different needs and environments (Wood 1997).

The framework divides policies into three categories. First, organisational policies, which require changes in the organisational structure. Second, operational policies, which require developing work practices to help compliance. Third, technical policies, which require changes to the IT infrastructure.

All of policies are affected by the context 'environment' in which they operate. The context consists of external factors e.g. regulations, and internal factors e.g. socialism and management. The security policy process depends on the cultural acceptance and the reinforcement within the organization.

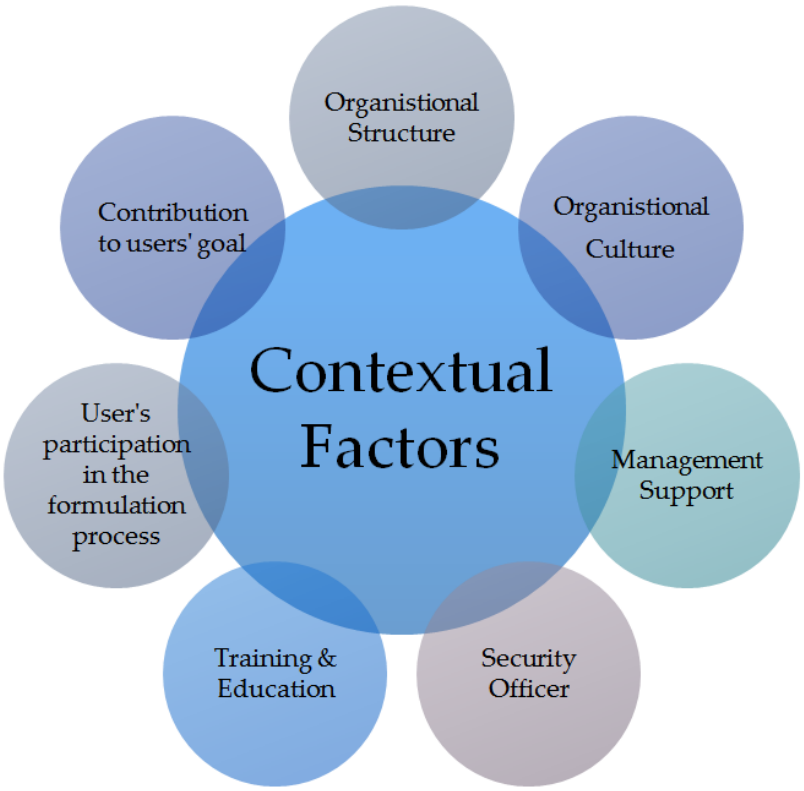

Figure 1. The Contextual Framework

2.7 Information Security Policy Compliance

Siponen, Muhamood and Pahnila (2010) identified two forms of compliance; intention compliance and actual compliance; and identified major factors that influence the compliance of information security policy stated in table 1. Their research showed that the factors of normative beliefs, threats appraisal, self-efficacy, and response-efficacy and policies visibility affects employees' intention; while deterrence and rewards affects employees' actual compliance. However, it is important to note that research showed that rewards and response-efficacy were of an insignificant impact on actual compliance.

Table 1 (Siponen, Muhamood and Pahnila 2010)	
Normative Beliefs	Social pressure.
Threats Appraisal	Estimations and assessment of threats that can be faced.
Self-Efficacy	One's ability in complaining with policies.
Response-Efficacy	Ability of security team and policies in handling threats.
Policies Visibility	Policies are advertised and made transparent in the organisation.
Deterrence	Penalties, social disapprovals and psychological punishments for non-compliance
Rewards	Rewards for compliance.

2.8 Accountability and Responsibility

It is critical to adopt security policies that outline the accountability and the responsibility regarding the protection of information assets, as the consequences for failing to do so can be significant (Ward & Smith 2002). Therefore, there must be security policies to define the rules, responsibilities and the accountability of individuals regarding the protection of information assets.

2.9 Policy Analysis, Assessment and Refinement

Due to the dynamic nature of security policy and the frequent changes that occur in the organisation's environment such as technological changes, security policy is deemed to be a continuous and on-going process (Karyda, Kiountouzis and Kokolakis 2004; Rees, Bandyopadhyay & Spafford 2003).

As a result, the PFIRES life-cycle model in figure 2 is developed to aid the analysis, assessment and refinement of security policies to ensure their continuous alignment with organisational objectives (Rees, Bandyopadhyay & Spafford 2003).

This model is an iterative process, benefits from continuous feedback and consists of four main phases. First, the access phase involves the creation or the adjustment of polices according to the analysis of the risks associated with information assets. Second, the plan phase includes the planning of suitable security strategy and policy that is in line with business requirements, and in defining the technical requirements that support the security policies. Third, the deliver phase is the implantation of the policy and includes defining and implementing the controls. This includes designing and selecting the infrastructure's best components consisting of practices, procedures and mechanisms; and implementing them. Finally, the operate phase is the daily management of polices through enforcement and monitor methodologies; and reviewing external and internal trends that may require the re-initiation of PFIRES.

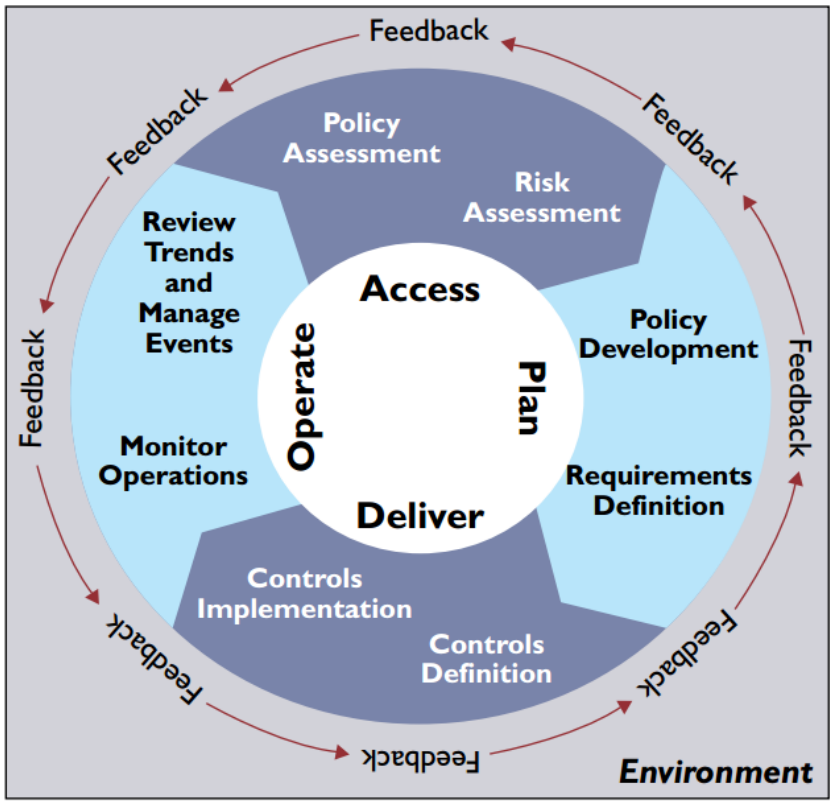

Figure 1 PFIRES Framework (Rees, Bandyopadhyay & Spafford 2003, p102).

2.10 Legislations Ambiguity

Legislations themselves can cause ambiguity. The HIPPA act permits the release of EPRs without the individual's authorisation in special circumstances such as controlling disease, injury or disability. The issue lies with 'what exactly is a special circumstance' (Garfinkel, Gopal & Thompson 2007; Lending 2010).

2.11 Secondary Users

The most common type of threat to the confidentiality of EPRs is somehow different. The threat here is the uncontrolled secondary use of EPRs. Secondary users include pharmaceutical companies and insures. These secondary users are authorised to access EPRs for medical purposes, however, once they have access to EPRs, they can disclose EPRs for other undesirable purposes (Rindfleisch 1997). Moreover, the law allow secondary users to access EPRs without the authorisation of individuals such as self-insured employers. (Anderson 2000; Garfinkel, Gopal & Thompson 2007; Rindfleisch). Healthcare organizations need to cater this human factor issue to preserve the privacy of EPRs (Cannoy & Salam 2010).

2.12 Health Care Systems

Healthcare organisations implement and use distributed and decentralised systems, to facilitate the sharing of EPRs for many benefits such as improving the healthcare quality (Smith & Eloff 1998). For example, a nurse can regularly update patient's EPRs on a system, and the doctor can access and

monitor the patient more efficiently and effectively and can give directions online. However, security concerns and issues revolve around the preserving the confidentiality of EPRs such as the secondary uncontrolled use of information and law enforcement (Anderson 2000; Rindfleisch 1997). Figure 3 demonstrate in a holistic view the distributed systems and the various entities that communicate with each other (Smith & Eloff 1998).

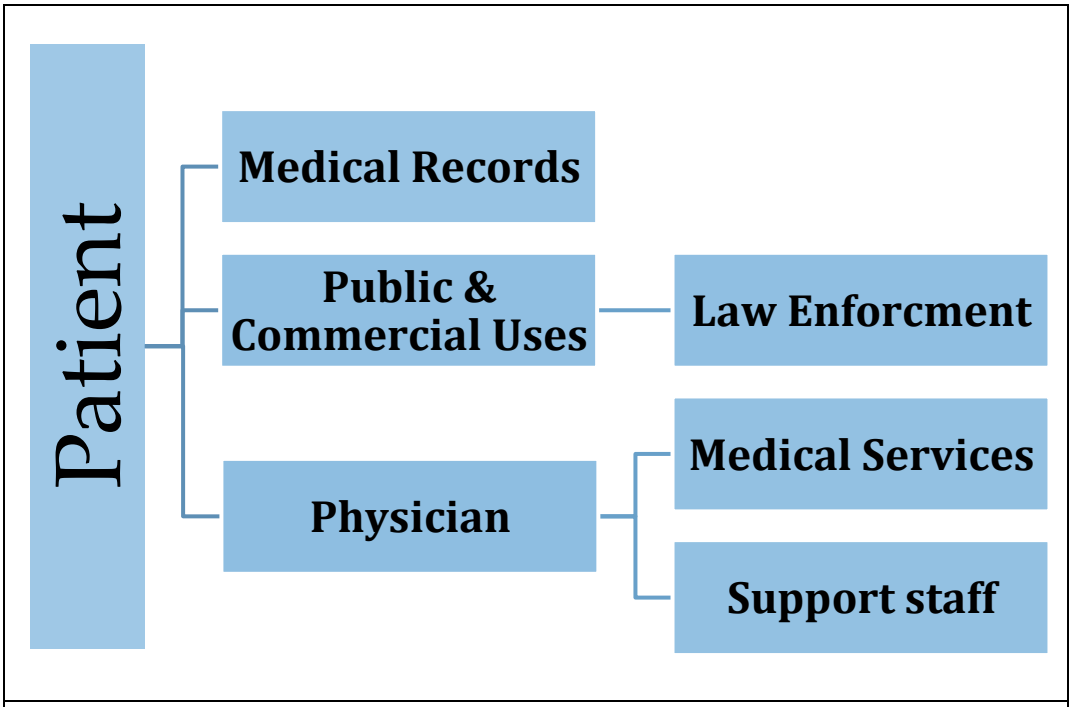

Figure 3 Distributed Systems and Entities

2.13 Absence of widely adopted software applications

There is a lack of support from key vendors in providing commercial systems that can facilitate sharing EPRS while preserving their confidentially. Most of the developed systems are made by academic healthcare researches or by small-scale specialised vendors; and these system are usually developed to suit specific and unique purposes. (Anderson 2000; Hoffmann 2009).

2.14 Standardisation and Interoperability

The lack of widely adopted EPR systems, cause one significant difficulty, which is the issue of protocols and standards. This creates a chaotic situation in terms of having conflicting, rigid, inconsistent and very varying standards and protocols to collect, share, store and retrieve EPRs (Gaunt 2000). Therefore, complexities are faced in terms of linking and maintaining interoperability and flexibility between the legacy systems of the various healthcare organisations, which ultimately effect preserving the confidentially of the EPRs (Hoffmann 2009). Various techniques have been developed in the literature to overcome this issue e.g. the Individual Identifiable Micro-data Technique (Garfinkel, Gopal & Thompson 2007).

2.15 Individually Identifiable Micro-data (IIM) Technique

Individual Identifiable Micro-data (IIM) Technique is used as a categorisation standard that use different levels of data set attributes of patient health information as a preventative measure to preserve the confidentiality of EPRs. This technique help in the collection and dissemination of EPRs

among different entities 'internal and external entities', while maintaining the confidentiality of individuals by only revealing minimal information required for processing, thus preventing unnecessary access to unrequired parts of the sensitive information in EPRs (Garfinkel, Gopal & Thompson 2007).

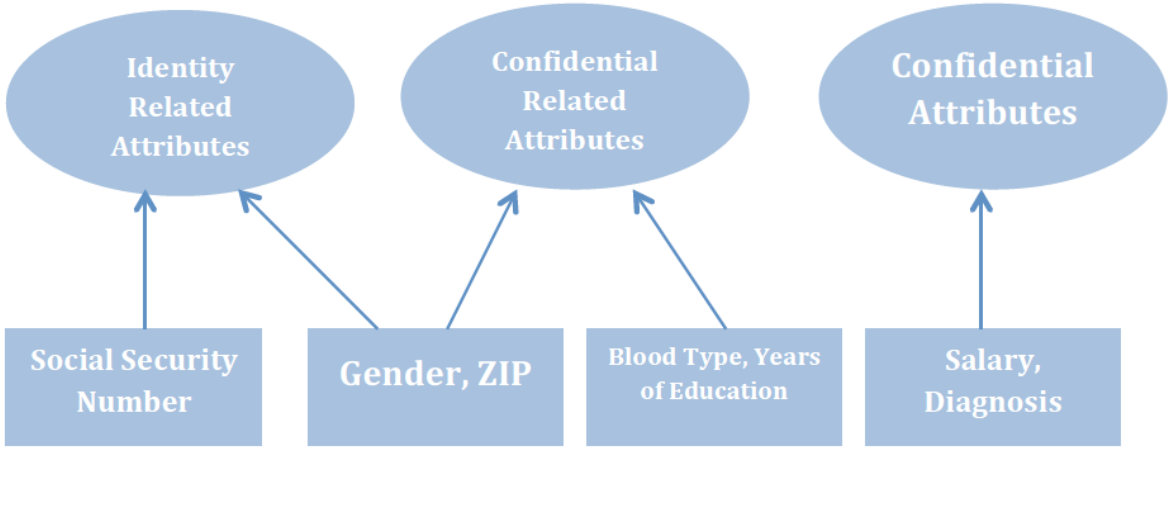

Figure 4 IIM Technique (Garfinkel, Gopal & Thompson 2007, p24).

As shown in figure 4, the attributes contain information of varying sensitivity. Information falling under identity-related attributes such as patient's name is highly confidential, while information falling under confidentially-related attributes such as blood-type is less confidential and so on.

This technique also provides the advantage of using un-identified health information for statistical proposes. Organisations seeking competitive advantage such as drug improvements through statistical studies can view patients information e.g. age without compromising the confidentially of the patients e.g. name (Garfinkel, Gopal & Thompson 2007).

Furthermore, an important aspect about IIM technique is the possibility of grouping and merging ERPs data sets that tracks back to one patient or more. This can greatly increase the privacy of patient(s) sensitive information by using the concept of abstraction as shown in figure 5.

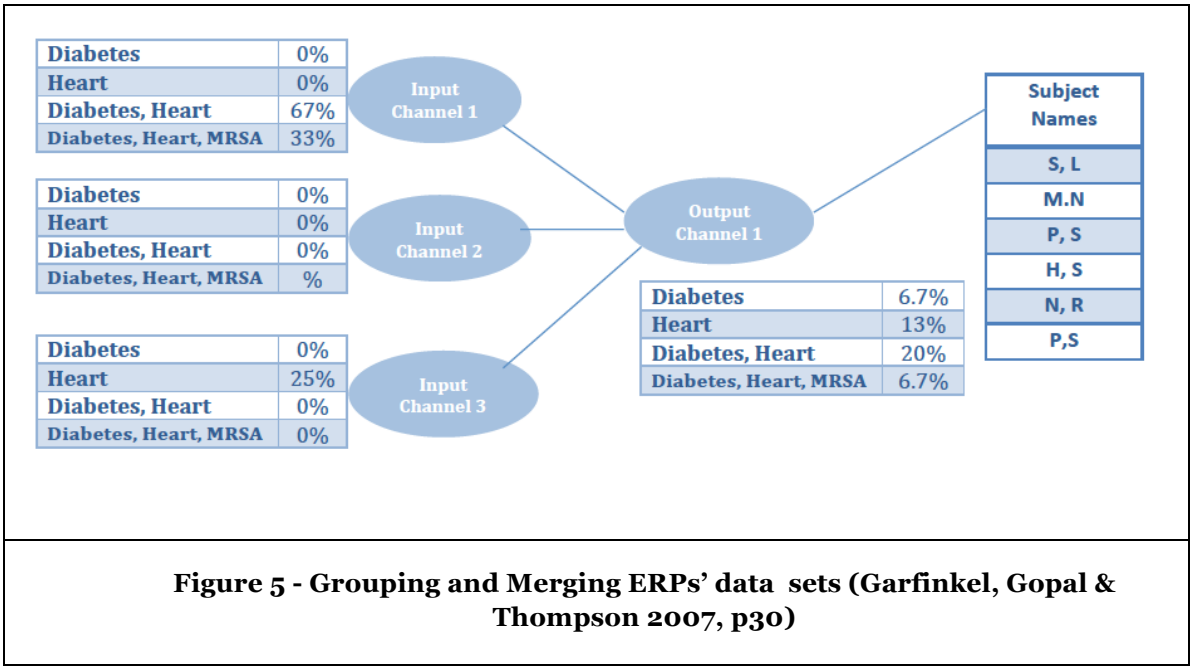

Figure 5 - Grouping and Merging ERPs' data sets (Garfinkel, Gopal & Thompson 2007, p30)

Figure 5 shows an example of IMM technique in use. Entity(s) querying patient(s) EPRs can only see the result of their input channel 'query' and can only track back to the output channel 'the available list of patients' names'. Moreover, these queries can be controlled by the underlying logic of the software that is also governed by security policies , e.g. different access privileges for input channel 1.

2.16 The ETHICS Method

The ETHICS method of soft systems engineering is a user extensive approach in order to create, refine and enforce information security policies to preserve the confidentiality of EPRs. This includes enforcing security compliance in employment agreements, extra confidentiality agreements, training programs and introducing security policies (Gaunt 1998).

ETHICS acknowledges the importance of including the input of various users in the planning and the implementation, therefore it engage people with different expertise; IT, business, health expertise etc. to help creating and refining security policies.

ETHICS is an on-going process that includes continuous refinement, and may require some time in order to demonstrate its effect. It requires senior management commitment, good leadership and continuous participations of the involved users (Gaunt 1998).

2.17 Information Assurance (IA) Policy Compliance Framework

The IA framework aims at addressing employees' behaviour including attitudes and believes, by providing a supportive environment, to help them comply with security policies in order to preserve the confidentiality of EPRs (Cannoy & Salam 2010). The framework includes three sequential main phases causing chain effect that lead to policy compliance. The first phase discusses external factors that acts as a base to support developing the next two phases; believes and attitudes. The external factors include government regulations, cultural awareness and training programs etc. Figure 6 demonstrate the IA Policy Compliance framework.

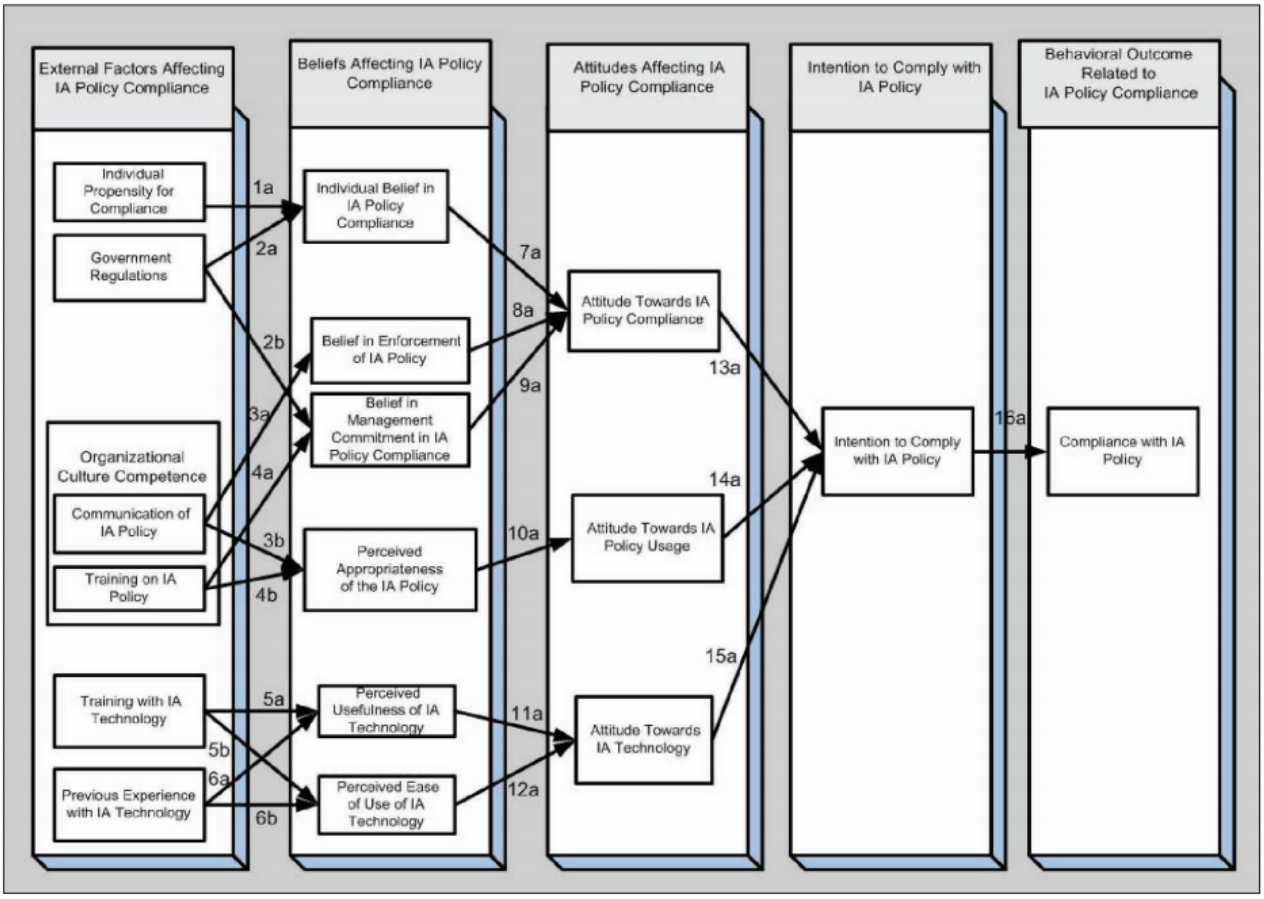

Figure 6 IA Framework (Cannoy & Salam 2010, p128).

3. Methodology section

The security policy's perspective on preserving the confidentiality of EPRs' has been developed by conducting a literature review only from high quality journals. There are twelve papers ranked A and A+ by the Australian Council of Professors and Heads of Information Systems from the following journals:

- Journal of the Association for Information Systems
- MIS Quarterly
- Communications of the ACM
- International Journal of Medical Informatics
- Journal of Computer Information Systems
- Information Systems Research

Further, three papers were ranked A and A+ by the Australian Research Council from the following journals:

- *American Journal of Law and Medicine*
- American Journal of Public Health
- Information Systems Journal

The search engines of Melbourne University Library and Google Scholar were used to search the papers using the following keywords: Health confidentiality, Patient privacy, Patient information security, EMR security, Health Information Security Policy, health confidentiality behaviour, health data privacy.

Of 25 articles that were found, only 15 articles were relevant, which focused on the following themes: security concepts within the healthcare industry, policy compliance, policy creation and refinement and policies regarding technology geared towards preserving the confidentiality of EPRs.

4. Discussion

Based on the above literature review, healthcare is one industry where, a minute mistake of information will bring in life changing situations. So the deterministic factors of EPR would be obtaining and sharing accurate data, while sharing data becomes complex in EPR's, where certain level of privacy and authorization have to be maintained.

Security policies will help in preserving the confidentiality of EPRs, not just as a rulebook or with a technology, instead as a collective measure of flexible and inflexible policies, with a technology to support, along with continuous process of SETA programs, monitoring and reinforcement and all these to be done through the power of top management. This flexibility will play a key role in a large, multi-culture or multinational healthcare organization.

The objective would be attaining highest possible confidentiality, with very less risk level, but also obtaining a trade-off between data utilization and confidentiality. Data utilization refers to EPRs being used by various entities for different purposes.

In preserving the confidentiality of EPRs, security policy creation, refinement and adoption are the most important criteria to be addressed; also attitude of the employees towards EPRs security and their compliance with security policies plays a key role.

4.1 The IIM Technique

The Technology:

The IIM technique has a huge potential of delivering high privacy with reduced risk, particularly with the involvement of secondary users. The inclusion of identity information forms the key. Though the technology offers a high standard of privacy it also possesses few information security policy issues, which will be discussed in the following sections.

Classification of Information

The necessity of EPR's is to provide information to practitioners for diagnosis, information to insurance company people who cover the patients and secondary users like pharmaceuticals to provide medicines and statisticians who conducts research for finding patterns. Different people require different information; confidential information for a medical practitioner might seem less confidential for a pharmacist. IIM helps us in forming output channels and grouping them into sets, which will provide the power of controlling information flow. So balance has to be achieved in creating security policies that cater the classification of information and risk factor associated to it.

Trade-off (EPRs - Utilization vs. Confidentiality)

Confidentiality of the EPRs when distributed has to be negotiated with the amount of information delivered. The right data with the right subset has to be sent at very low risk. The lesser the risk factor with possible maximum amount of required information will increase the efficiency in preserving EPRs confidentiality. To achieve this trade-off, selection of data set plays a key role. Complex strategies have to be involved in selecting the data sets of an EPR. Security policies have to be developed in such a way that the selection criteria are formulated and provides scope for future modifications.

Maturity of the Organization

The implementation and the governance of IIM require very high level of maturity of information security policy appreciation within the organization, along with excellent mixture of knowledge including IT, medical and management skills; in order to effectively and efficiently implement security policies to preserve the confidentiality of EPRs in this technique. The top management should understand the necessities of this method, which will help in enforcing security policy in the top-down format. Without the top management's supporting enforcing the policy to the lower order employees is very tough. The attitude of employees towards security is hugely dependent on top management's attitude towards the confidentiality of EPRs.

Legislation Ambiguity

Predicting and picking the data sets involves high complex decision-making, improper decisions will lead to security breach. So decision-making has to be dealt with proper care and with deep insights, which can be done by developing operational policies under control phase.

Apart from this, the complexity exists within legislation by itself; the confidentiality is not really properly defined under law, this will hinder the process of policy formation. What is termed as confidential has to be identified and based on that policies have to be developed to preserve the confidentiality of EPRs.

Distributed Systems and Standardization

The level of complexity will be skyrocketed, when EPRs has to be shared with different organizations 'other systems' using IIM technique. When security policies to preserve EPRs confidentiality are developed, they are not just for the primary institutions and users but also to secondary institutions such as contractors, insurance company, pharmaceuticals, etc. This also includes catering for the human factor and the technical infrastructure within each involved organization e.g. standardization in SETA programs, firewalls, security applications and mechanisms etc. Additionally, when changes occur to security policies at one system, this can affect polices at other system(s) as well, hence a network of maintained, interconnected and mutually adopted organizational, operational and technical security policies; which will work together to preserve EPRs confidentiality.

New Legislations

If new legislations or new changes to the current legislation occur regarding EPRs confidentiality, this can cause significant implications on the overall structure of security policies, and can impact all types of policies. This is due to the fact that the nature of the IIM technique requires great amount of planning and can involve high complexity as discussed above. Therefore, a small change in security policies can result in major implications.

Cost Associated

The usual mind-set of organizations that Information Security is luxury expenditure will not help in implementing IIM technique and the security policies to govern it. The organization should

understand the necessity of information security policies associated with such model, which will provide competitive advantage over their competitors. The cost associated in implementing this methodology is very high, like the technology involved, software, training associated. Implementation of these can be scaled up from large organizations to small organizations. Small organizations may not need such sophisticated technology, with such major implications on information security policy and the human factor.

Data Accuracy

As discussed in the literature, data accuracy is of significant impact on the compliance of users towards preserving the confidentiality of EPRs. Thus, classification of data is another complex methodology involved; high sensitive data should be identified and classified under high sensitive datasets. Security policies should be able to provide guidelines on classifying highly sensitive, sensitive and non-sensitive EPRs data sets. The policies will involve proper training for the users to classify the confidential data sets within an EPR, and in grouping them accordingly. This relies mostly on operational and technical polices, however organizational policies are also required e.g. cultural awareness.

4.2 ETHICS Method

The ETHICS method includes an excellent environment that facilitates in creating the most suitable security policies; and in ensuring their continuous refinement, as it relies heavily on user involvement including IT, business, and healthcare experts etc. Also top management commitment and leadership of the healthcare organisation is considered to play a key factor in managing the ETHICS method.

Thus, the creation and refinement of security policies regarding persevering the confidentiality of EPRs, is conducted on much more higher level of effectiveness and efficiency and giving proper consideration for aspects such as 'internal and external factors'. Moreover, this method can tackle the issue of secondary users much more efficiently, due to its social alignment nature e.g. social pressure, fast policy refinement etc. However, there are some issues associated with the ETHICS method as in the following;

Lack of Proper Guidelines

ETHICS method just gives general description of how it works. The absence of proper guidelines can lead to problematic situation that can affect the confidentiality of EPRs; particularly when its nature is very user extensive and lots of views and opinions are involved. For example, which view(s) to undertake in policies, is there a criterion? what is the organisational hierarchy? It is not clear. Further, it does not address any guidelines that set accountabilities and responsibilities of people involved, which can lead to severe consequences.

Additionally, the lack of proper guidelines rise further concerns about the actual forms of security policies e.g. simplicity, attractiveness, fit culturally etc. 'simply referred at as policies about policies'. Such concerns can be further complicated when various cultures are involved. Finally, the method lacks proper guidelines for security compliance and this is a critical aspect.

Massive Influx of EPRs

Due to the intense social alignment nature of the ETHICS framework, in the case of large organisations were there is a significant influx of EPRs circulating through many departments or even organisations, this method can create a chaotic situation in terms of formulating the most suitable security policies to preserve EPRs confidentiality. Therefore, this method requires need excellent leadership skills and knowledge to handle such situations.

Resource Intensive

The lack of proper guidelines, and the chaotic situation that can occur from a significant influx of EPRs; will require additional activates in order to compensate for these issues. Even the nature of the ETHICS method can hinder the functionality of the human factor. As a result, the ETHICS method when not managed and governed properly, it can be resource intensive; which can negatively impact preserving the confidentiality of EPRs.

ETHICS vs. PFIRES

In terms of preserving EPRs confidentiality, the ETHICS method demonstrate robustness when it comes to creating the most suitable organisational and operational security policies and how to cater for them in terms of cultural awareness and acceptance. However it does not tackle technical polices quite well and how to cater for their requirements. The PFIRES framework demonstrates more robustness in terms of tackling the requirements of technical policies, because it includes guidelines such as requirement definition and documentation.

4.3 IA Compliance Framework

The IA compliance framework will help in adopting and taking security policies to the bottom level; and in effectively enforcing them using methods such as SETA programs. According to the literature, this is very well focused framework that tackles the intention and the actual compliance of users towards preserving the confidentiality of EPRs.

Excellent in Compliance, but Nothing More!

It is important to note that the literature showed that the policy process is on-going process, and so as adoption, 'hence compliance'. Although this framework demonstrates excellent catering for policy compliance regarding the confidentiality of EPRs, it seems that it only addresses the gap between policy implementation and refinement; and cannot act independently. This framework by itself creates disconnect between the implementation and the refinement of security policies. Therefore it must be integrated with other framework/method to demonstrate effect.

5. Future Research Opportunities:

5.1 Research Opportunity One

IIM Trade-off (EPRs - Utilization vs. Confidentiality)

As discussed, the issues surrounding this trade-off and the likelihood of developing the best security policy module with the possibility of further improvements to the technique itself to tackle or limit the effect of this trade-off. This can help in further maximizing the confidentiality of EPRs, particularly when multi systems and many different users are involved. Developing security policies to tackle this trade-off can act as a standard to govern this technique; this can also help in creating and adopting a standard for sharing EPRs. This provides a scope for further research in this area.

5.2 Research Opportunity Two

ETHICS Method - Lack of Proper Guidelines

As discussed, the lack of detail and robust guidelines in the ETHICS methodology, will affect the perceived view of the overall effectiveness, due to the issues mentioned such as security policies regarding responsibility and accountability. The lack of proper guidelines can be a further research opportunity to enhance the ETHICS method; to act as a much robust security policy mechanism that

help in preserving EPRs confidentiality and most importantly, encountering the issues of secondary users.

5.3 Research Opportunity Three

PFIRES Framework, Ethics Method and IA Framework Mergence

Due to the unique nature of the healthcare industry and unique issues such as secondary users as a threat within the healthcare industry, there is a strong opportunity in further enhancing the PFIRES framework and tailoring it out to be well equipped towards the formulation, implementation, adoption and re-formulations to greatly help in preserving the confidentiality of EPRs. This enhancement can be adopted from the emergence of ETHICS method and the AI compliance framework with the PFIRES framework.

The ETHICS method can significantly enhance the access and plan phases to be more suitable, regarding the formation and refinement of security policies that are better focussed towards the confidentiality of EPRs. Moreover, the IA framework can help greatly in maximizing the enforcement of security policies, and can further enhance the operate phase.

Such merging can provide deeper insights and will help in obtaining high control in terms of preserving the confidentiality of EPRs. This whole approach will help to develop policies which are powerful and that can govern and evolve along with time. However, this needs to be researched, developed and tested to be proving effective.

6. Conclusion

The paper encompasses study on learning security policies associated with security modules and mechanisms that are geared towards achieving confidentiality in EPRs, which has been victimized for information breach very often. This paper first, defined the concepts involved around EPRs and how to formulate policies that will be efficient in the EPR atmosphere. Second, IIM methodology with proper security policies is found to be satisfying the necessity criteria of achieving high confidentiality at the same time allowing classified information for different requirements at different instances by different people with reduced risk levels. Also, different frameworks are analysed, for instance the PFIRES's framework, ETHICS method and IA Compliance framework.

Later Study advanced in identifying which is more effective in the EPR setup and it was identified that user extensive approach would be the best-suited approach. After further analysis it was identified that, ETHICS method was more suitable on formulating and refining policies, while IA Framework was deep into enforcing the security policies. And IIM the technical part, provided the required high confidentiality; so it was learnt that, the mixture of these three with the PFIRES framework can be a well suited model for formulating Security Policies on achieving confidentiality in EPR's. However, few issues were discussed that are found with these modules and mechanisms that can impact the security policies associated with them that can affect preserving the confidentiality of EPRs

Finally, three different opportunities for further research was identified that can assist in further enhancing the security modules and mechanisms of preserving EPRs confidentiality, which will lead to detailed discussions.

7. References

Anderson, JG 2000, *'Security of the distributed electronic patient record: a case-based approach to identifying policy issues'*, International Journal of Medical Informatics, vol. 60, pp. 111 – 118.

Angst, CM & Agarwal, R 2009, *'Adoption Of Electronic Health Records In The Presence Of Privacy Concerns: The Elaboration Likelihood Model And Individual Persuasion'*, MIS Quarterly, vol. 33, no. 2, pp. 339-370.

Bulgurcu B, Cavusoglu H & Benbasat, I 2010, *'Information Security Policy Compliance: An empirical Study of Rationality-Based Beliefs and Information Security Awareness'*, MIS Quarterly Publish, vol. 34, no. 3, pp.525-548.

Cannoy, SD & Salam, AF 2010, *'A framework for health care information assurance Policy and compliance'*, Communications of the ACM, vol. 53, no. 3, pp. 126-131.

Devargas, M 1995, *'The Total Quality Management Approach to IT Security'*, NCC Blackwell.

Dillon, TW & Lending, D 2010, *'Will They Adopt? Effects of Privacy and Accuracy'*, Journal of Computer Information Systems, vol. 50, no. 4, pp. 20-29.

Garfinkel, R, Gopal, R & Thompson, S 2007, *'Releasing Individually Identifiable Microdata with Privacy Protection Against Stochastic Threat: An Application to Health Information'*, Information Systems Research, vol. 18, no. 1, pp. 23–41.

Gaunt, N 1998, *'Installing an appropriate information security policy'*, International Journal of Medical Informatics, vol. 49, pp.131 – 134.

Gaunt, N 2000, *'Practical approaches to creating a security culture'*, International Journal of Medical Informatics, vol. 60, pp. 151–157.

Greenaway, KE & Chan, YE 2005, *'Theoretical Explanations for Firms' Information Privacy Behaviors'*, Journal of the Association for Information Systems, vol. 6, no.6, pp.171-198.

Hoffmann, L 2009, *'Implementing Electronic Medical Records'*, Communications of the ACM, vol. 52, no. 11, pp.18-20.

Höne, K & Eloff, JHP 2002, *'What Makes an Effective Information Security Policy?'*, Department Computer Science, University of Pretoria, South Africa.

Hughes, M & Stanton, R 2006, *'Winning security policy acceptance'*, Computer Fraud & Security, no. 5, pp. 17-19.

Karyda M, Kiountouzis E & Kokolakis S 2004, '*Information systems security policies: a contextual perspective'*, Elsevier publish, vol. 24, pp. 240- 260.

Katsikas S, Lopez J, Backe M, Gritzalis S & Preneel B 2006, '*Information Security'*, Springer-Verlag Press, Berlin Heidelberg.

Myers, J, Frieden, TR, Bherwani, KM & Henning, KJ 2008, *'Privacy and Public Health at Risk: Public Health Confidentiality in the Digital Age', American Journal of Public Health,* vol. 98, no. 5, pp. 793-801.

Rees, J, Bandyopadhyay, S, Spafford EH 2003, *'PFIRES: A Policy Framework for Information Security'*, Communications of the ACM, vol. 46, no. 7, pp. 101-106.

Rindfleisch, TC 1997, Privacy, *'Information Technology, and HealthCare'*, Communications of the ACM, vol. 40, no. 8, pp.93-100.

Rodwin, MA 2010, '*Patient Data: Property, Privacy and the Public Interest'*, *American Journal of Law and Medicine*, vol. 36, pp. 586-618.

Siponen M, Mahmood M & Pahnila S 2010, '*Compliance with Information Security Policies: An Empirical Investigation'*, IEEE Computer Society Publish.

Siponen M, Mahmood M & Pahnila S, 2009, *'Are employees putting your company at Risk by not following information security policies?'*, Communications of the ACM, vol. 52, no. 12, pp. 145-147.

Smith, E & Eloff, JHP 1998, *'Security in health-care information systems —current trends'*, International Journal of Medical Informatics, vol. 54, pp. 39 – 54.

Stahl, BC, Doherty, NF & Shaw, M 2012, *'Information security policies in the UK'*, Information Systems Journal, vol. 22, pp. 77-94.

Ward, P and Smith, CL 2002, *'The Development of Access Control Policies for Information Technology'*, Systems Computers & Security, vol. 21, no. 4, pp. 356-371.

Wartenberg, D & Thompson, WD 2010, *'Protecting Privacy or Protecting the Public'*, American Journal of Public Health, vol 100, no. 3, pp.407-412

Wiant, TL 2005, *'Information security policy's impact on reporting security incidents',* Computers & Security, vol. 24, pp. 448-459.

Wood, C 1997, '*Policies Alone Do Not Constitute a Sufficient Awareness Effort'*, Elsevier Science Ltd Press, Canada.

Wood, C 2000, '*An unappreciated reason why information security policies fail'*, Computer Fraud & Security, no. 10, pp.13-14.

Author/s:
Alateeq, Sulaiman; Viswanathan, Hari Hara Sudhan; Fuentealba, Christobal; Pang, Haoran; HU, CHENWEI; Salisbury, Sean

Title:
Confidentiality and health: a literature review

Date:
2013

Citation:
Alateeq, S., Viswanathan, H. H. S., Fuentealba, C., Pang, H., Hu, C., & Salisbury, S. (2013). Confidentiality and health: a literature review. Melbourne, The University of Melbourne.

Publication Status:
Unpublished

Persistent Link:
http://hdl.handle.net/11343/33344

File Description:
Confidentiality and health: a literature review