A model for information security compliant behaviour in the healthcare context

Debra Box\textsuperscript{a}, Dalenca Pottas\textsuperscript{a}

\textsuperscript{a} School of ICT, Department of IT, Nelson Mandela Metropolitan University, Port Elizabeth, 6001, South Africa

Abstract

Healthcare professionals are dedicated to maintaining the confidentiality of patient information but are resistant to maintaining an information security compliant environment within a health information system. In this paper, a literature review is used to gain knowledge about the factors that affect this information security compliance. An overview of the security threats and those specific to healthcare is presented. The information security misuse deterrence and compliance promoting factors that affect information security compliant behavior are identified. Their role in strengthening information security compliant behavior is examined. The information security compliance model is introduced and its part in fostering compliant security behavior is reviewed. Its components comprise a body of knowledge, skills and attitude, and behavioural intervention, together with the misuse deterrence and compliance promoting factors. The application of the model is intended to instill, within the user, an attitude that is more conducive to information security compliant behaviour in the healthcare context.

Keywords: Healthcare Information Systems Management; Information Security; Data Security & Protection; Healthcare Content Management

1. Introduction

The use of Information Technology (IT) has become prevalent within the healthcare environment. The pattern of initially automating mundane tasks by information systems is repeated in the healthcare industry [1]. The earliest successes of IT adoption, in the healthcare industry, were business function applications. Non-business functions remained under-developed until the Nineties when emergent Information Communication Technology (ICT) enabled the development of integrated Health Information Systems (HIS).

The impetus to strengthen HIS is driven by international bodies, the United Nations and the World Health Organisation. The United Nations, in 2000, adopted the Millennium Declaration. The focus of the World Health Organisation is to strengthen HIS to support the Millennium Development Goals. There are few countries with
sufficiently strong HIS in place to adequately monitor their progress towards these goals. The need for better health information arises from the need to assure evidence-based decision-making and improve accountability [2].

Organisational information is viewed as a business asset and a commodity that requires protection. The goal of Information Security (InfoSec) is to ensure a sustainable and adequate level of security or protection for these information assets [3].

Computer applications in the healthcare industry threaten the InfoSec of the patient information whilst they provide and offer significant benefits to both patients and practitioners. The electronic patient record is more vulnerable to disclosure and tampering than the paper-based form [4].

Current literature recognizes that users pose a security challenge due to their ignorance, mistakes or deliberate acts. This is supported by recent survey reports and anecdotal evidence [5]. The role of user security behaviour is increasingly recognised as a focal point in the study of InfoSec compliance [6].

Success, according to [5], is more likely when the organization invests in both technical and socio-organisational resources. However, there is an imbalance in investment in technological safeguards when compared to that in human controls such as continuous InfoSec education and awareness programs [7].

The existing clinical culture exhibits a variety of attitudes to the role of IT in healthcare. Practitioners are encouraged by the advances in clinical computing and see technology as capable of increasing their efficiency and the quality of care provided. One concern is the task overhead imposed by complying with InfoSec measures [8]. Healthcare professionals, through their professional skills and unique operating environment, accentuate their singular InfoSec challenges.

There is scarce empirical research into IT use in the healthcare environment. The longitudinal study into HIS acceptance by [9], as reviewed by [10], reveals that apathy and passive resistance morphed into aggressive resistance behaviours. This highlights the need to address the issues that prevent the implementation of HIS and its subset, Health InfoSec. A means of motivating InfoSec compliance is needed [10]. There are many factors that contribute to compliance and non-compliance [11]. These need to be identified and appropriately organised to improve user acceptance and by association, InfoSec compliance. The identification of motivators for InfoSec compliant behaviour is seen as central to expanding the literature in InfoSec and to define the focus of mechanisms to improve user compliance.

This paper is organised as follows. In section 2 the research method is described. Section 3 presents the results of the critical literature review. InfoSec and specifically Health InfoSec are addressed. Threats specific to both are examined. Factors that affect InfoSec compliance are discussed. Finally, in section 4 - the discussion, the Information Security Compliance Model (ISCM), as the proposed solution, is reviewed and its proposed effect on compliance is examined. The paper ends with section 5, the conclusion which reviews the results, contributions for research and practice and suggestions for future research.

2. Methods

This research is based on the design science research strategy. The result is a purposeful IT artefact produced to resolve a unique, important organisational problem [12]. The problem being investigated is the trusting and co-operative nature of health professionals, which leads to apathetical behaviour towards InfoSec [10]. The research questions under review are, in the healthcare environment, what motivational and behavioral factors affect InfoSec behavior? What comprises an InfoSec culture? How does the medical culture affect InfoSec behavior? What ISCM components will improve InfoSec behavior?

A variety of secondary data sources are investigated to understand the problem domain. The databases used include Masterfile Premier; Academic Search Complete; Medline; Business Source Complete; Science Direct; Emerald; Biomed and Pubmed Central. The search criteria include InfoSec and/or Awareness; HIS, Security Culture; Medical Culture, Information Security AND Healthcare; Behavioural Change Agents AND/OR Behavioral Interventions. The search phrases InfoSec, InfoSec Awareness AND Healthcare returned a limited number of articles in the healthcare context. Results returned for InfoSec and electronic health records were excluded because they relate to aspects beyond the research questions. A suitable ISCM is identified through iteration, evaluation and theory justification using logical reasoning and argumentation.
The search results provide the contextual environment in which a qualitative content analysis was performed according to the methods endorsed by [13,14]. Concepts or factors, relating to the research questions, appear throughout the search results. The aim of a content analysis is to attain a condensed and broad description of the phenomenon that is replicable and valid. The outcome is descriptive concepts [13].

Both deductive and inductive content analysis methods are used. The research questions lead the deductive analysis which examined the existing research and provided direction towards both theories and concepts applicable to an ISCM. Inductive content analysis was used to specifically adapt these concepts and theory to the area of InfoSec in the healthcare environment where there exists limited available literature. Subject-specific factors emerged as themes or categories as the content analysis process continued.

The credibility of research findings deals with how well the categories cover the data. It is important to make defensible inferences based on the collection of valid and reliable data. The reliability of the study is based on demonstrating a link between the results and the data [14]. The author proposes that, in this curtailed format, sufficient defensible inferences and links between the results and data are made.

3. Information Security Compliance

Information security compliant behaviour, whether generic or within the healthcare environment, is a combination of many components. The goals of InfoSec and those specific to the healthcare environment are considered, together with generic and healthcare specific InfoSec threats. An overview of the factors which either deter or promote compliant behavior is presented. The various constructs in the ISCM are introduced; namely the Compliance Promoting and Misuse Deterrence factors; the Body of Knowledge; Attitude; Skills; Behavioural Intervention and Security Compliant Behaviour. This research holds that InfoSec compliant behaviour can be improved through the inter-relationship of these constructs.

3.1. The significance of health information

Health information holds the same significance as any other business information asset. It is described, by general consensus, as information about all the ‘resources, organizations and actors involved in the regulation, financing and provision of actions whose primary intent is to protect, promote or improve health’ [14]. Its importance is based, when using the functionality of ICT, on its ability to improve healthcare. There are a variety of reasons for strengthening HIS which include [15]:

- An increase in efficiency, productivity and service delivery;
- An increase in accountability;
- A reduction in healthcare costs and medical errors.

Health information filters up to the national level, therefore, the health information at the private practice level is as affected by the Millennium Development Goals as that used by government departments who determine the implementation of national health resources. The increased demand for quality health information has revealed the fragility of HIS.

3.2. Information security

Information security is the protection of information from a wide range of threats. This is achieved by managing a suitable set of security controls, policies and procedures within an Information Security Management System. The goal of general InfoSec is the ‘preservation of confidentiality, integrity and availability of information’ and includes such terms as the accountability of users, authentication, non-repudiation and reliability [3].

The reduction and mitigation of InfoSec threats has become a top managerial priority. However, organizations often rely on technology-based solutions. These help improve InfoSec but their excessive use seldom removes all the threats. Empirical and anecdotal evidence demonstrate that security incidents are increasing despite the progressive investment in technology-based solutions. This suggests that despite the technology-based measures implemented, there is little improvement in InfoSec compliant behaviour.
3.3. Health information security

The goal of InfoSec for health information is extended through the ISO 27799 standard and is stated as 'maintaining information confidentiality, availability and integrity (including authenticity, accountability and auditability)'. These goals carry extra weight when dealing with healthcare data, as any failures could, at worst, endanger the patient’s life or at least, reveal confidential data about the patient [16].

The focus of this research is the institution-based data source, namely the individual or personal health record of the patient and its InfoSec. The privacy of the patient is ensured by preserving the confidentiality of the personal health information which, in turn, is maintained by ensuring its integrity. Additional health considerations include compliance with data protection laws and privacy legislation, maintaining organisational and individual accountability and public trust in the healthcare provider and the HIS in use [16].

Patient health records contain all the information a thief needs to perpetrate identity theft. However, healthcare professionals are generally more concerned about protecting clinical information than their patients' identity information. Clinical data has layers of protection, such as computer passwords and other security features. The protection of identity information is not a natural thought process in the healthcare environment [4].

The status quo is reflected in the Global State of Information Security Survey 2014 which reports on various industries and presents a survey dedicated to the healthcare industry. A brief summary of the results note that 74% have confidence in the effectiveness of their security measures, however, only 22% have reviewed the effectiveness of their security measures. Security budgets remain at 2009 level. The detection of security incidents increased during 2013; however, the resultant harm to the patient record belies the 74% confidence in the security measures. 42% of security incidents are caused by current employees [17]. These results illustrate the continuing concern about InfoSec compliance within the healthcare environment.

3.4. Health information security threats

A new variety of threats are introduced through the use of automated HIS. The user represents a generic internal security-threat through the following acts which are a significant cause of security incidents [18]:

- A lack of common security sense or forgetting to apply security procedures;
- Users taking inappropriate risks due to ignorance of the risk involved;
- Deliberate acts of negligence or deliberate malicious acts.

Security threats posed by the users are classifiable along a continuum as illustrated in Figure 1.

![Fig 1. Information Security Threat Vector Taxonomy Abridged – Sourced [19]](image-url)
Internal sources of threats originate from the users who possess access privileges and intimate system process knowledge. Security policy violations range from passive – such as accidental incorrect data entry or carelessness, lack of motivation or poor training; volitional - such as voluntary rule-breaking by violating the InfoSec policy but without malicious intent - to intentional malicious non-compliance such as data theft or destruction, disclosing sensitive information or fraud [19].

Healthcare Information System specific threats are divided into three major categories; natural, human and environmental. Threats are grouped according to actions and consequences. Action types include destroy, modify, observe and emulate threat. Their consequences include disclosure, execution, misrepresentation, repudiation and integrity threats. Security threats are categorized as interruption, interception, modification and fabrication and are classifiable according to the type of asset involved. Threat agents are the authorized or unauthorized users and environmental factors. Threats originate from internal or external sources. Internal threats are based on user behavior which originates from ignorance, carelessness or maliciousness. External threats include software viruses or hackers [20].

3.5. Information security compliant behaviour strengthening

Information security compliant behavior is achieved through a variety of approaches. Research into strengthening InfoSec compliance, generally, focus on determining which factors cause user misuse or non-compliance.

One security measure proposed is to create an InfoSec Awareness culture by educating users about InfoSec risks and their responsibilities [21]. The implementation of an InfoSec policy and its alignment to business objectives is endorsed as a security-enhancing measure. 90% of large business respondents have a formally documented InfoSec policy in place [15]. InfoSec Obedience is seen as a means to ensure compliance because its premise is that user security behaviour reflects the vision defined in the corporate InfoSec policy [22]. User education about the necessity of security is proposed as a means to achieve this obedience [23]. Despite these measures, InfoSec compliance remains problematic [24]. These InfoSec strengthening measures comprise the Body of Knowledge construct in the ISCM.

3.6. Information misuse deterrence factors

The InfoSec community identifies the users as the ‘weakest link’ and avoids the ‘knowing-doing gap’ by using automated and mandatory InfoSec measures. The reasons these controls are ineffective and automated solutions fail include the following reasons [25]:

- Financial: organisations omit mandatory automated controls because the threat level is viewed as insufficient;
- Situational: organisations possess neither the infrastructure nor expertise to implement automated techniques;
- Technological: situations exist where full automation is impractical.

Much research is devoted to ascertaining the measures needed to prevent information system misuse and abuse which researchers envisage will improve InfoSec compliance. Organisations attempt to reduce Information System misuse, by implementing measures based on the general deterrence theory which include anti-virus software, access control schemes, the strict enforcement of security policies and fostering InfoSec awareness. Irrespective of these measures, the volume of computer abuse remains high [26].

Users view increased security measures as task or work stressors, privacy invasions, constraining and inconvenient. They feel compelled to maintain their operational performance whilst including the InfoSec measures in their daily tasks [8]. The responsibility for compliance with InfoSec policies rests with the user. For example, users who believe that increased InfoSec measures both restrict their work performance, and are counter-productive, are predisposed to be non-complaint [27].

Attributed trust is defined as the degree to which users believe they are trusted by the organisation. Individuals, who do not believe that their organisation trusts them, are unlikely to act in its best interests. The effect of introducing stringent InfoSec measures is a perceived lack of attributed trust towards the users which significantly increases internal user Information System abuse [28].
Many studies argue for the deterrence effects of sanctions. Sanctions are viewed as an important instrument to deter inappropriate behavior [5]:

- In criminology, individuals are viewed as amenable to sanction-based threats; therefore, the punishment-as-deterrence doctrine is widely accepted by policy makers and the general public;
- Sanctions are seen as important in the corporate world;
- Sanctions are highlighted as important to deterring computer security crimes;
- Sanctions are believed to lead users to perceive that there is a cost associated with non-compliance.

The users’ attitude towards compliance depends on the sanctions or consequences personally experienced. The perceived certainty and severity of sanctions moderate the intention to engage in deviant behavior [11,5].

Various researchers apply the general deterrence theory to InfoSec policy compliance, but with scant regard for the impact that emotions have on deterrence efficacy [19]. The research of [29] maintains that emotions affect attitude. The Coping Model of User Adaptation (CMUA) combined with Appraisal Tendency Framework is used in this research. Together they comprise the Behavioural Intervention construct. Together they provide the users with a variety of coping responses. The Appraisal Tendency Framework classifies four quadrants of emotion based on the users’ level of control: Loss; Deterrence; Challenge and Achievement. The Loss and Deterrence Quadrants reflect the event as a threat but over which the users feel that they have some control [29,10].

Coping is dependent on the users’ self-efficacy. Users claim to attempt to control a threat; however, a perceived lack of self-efficacy will negatively influence their decision to take preventative action [24].

The deterrence factors are, in the main, based on preventing computer misuse and abuse while envisaging that this will produce compliant behavior. To date, this approach is proven to be anecdotally and statistically unworkable. The corporate and research mind-set of using deterrence methods causes Motivating factors to be under-used. These information misuse deterrence factors comprise the Misuse Deterrence construct in the ISCM.

3.7. Information security compliance promoting factors

There are motivating factors which influence the user to exercise InfoSec compliant behaviour. The user requires a practical understanding of the InfoSec issues which are communicated through InfoSec awareness and education [18], and from external sources such as mass media, peers and social norms [30]. InfoSec education training and awareness programs and computer monitoring are positively associated with compliant behavior by the user [11].

Social influence and normative beliefs impact compliance which supports the belief that the expectations of superiors and peers exert a profound impact on compliance behavior [27]. This is relevant in the healthcare environment which is permeated with the ethic of trust.

Rewards alone, are not seen as effective in convincing users that InfoSec policies are mandatory, however, the specification of policies, evaluation of behaviour and computer self-efficacy are [5]. These organizational security policies, procedures and standards articulate the values and principals held towards InfoSec. These build the security values and attitudes of the users which are reinforced by the consistent behaviour of senior management and their peers towards these security values [18].

Self-efficacy is argued as the most persuasive mechanism of human agency which motivates and regulates individual behaviour. It is a form of self-evaluation which determines individual behavior. Computer self-efficacy is defined as the judgement of the individual about their capability to use a computer across multiple computer application domains. This is expanded to accommodate InfoSec and is redefined as Self-efficacy in InfoSec (SEIS). It appears ideally suited to InfoSec behaviour because self-regulation is critical in ensuring InfoSec [31]. SEIS is an element within the Skills construct.

Positive reinforcement about the benefits of IT, extending to InfoSec compliance, is advised. Positive emotions, identified in the Challenge and Achievement Quadrants in the Appraisal Tendency Framework, are a means to communicate the positive benefits accrued which, in turn, motivate constructive IT behavior and by inference, InfoSec complaint behaviour [29,10].

Attitude is defined, in the social psychological literature, as the relatively enduring evaluation of a given object. It includes beliefs (cognition), feelings (affect) and intentions about the object (conation). Attitude strength moderates the effect of user intention and compliance and it is measurable using personal relevance and related knowledge dimensions [11].
The sense of obligation between the employee and employer affects InfoSec compliance. This ‘psychological contract’ is viewed as an unwritten reciprocal agreement for both parties to act in each other’s best interest [18]. This is in alignment with the co-operative culture evident within the healthcare environment.

Organisational trust includes reputation, achievements and aspirations; and norms which form the trust bond, as exemplified by the quote ‘we all have a moral duty to abide by the law’ [26].

The moral judgement of the user is significant. A strong sense of moral judgement is an indicator of compliant behavior while the opposite holds true [11]. Moral motivation is regarded as an intrinsic incentive because users who believe their actions are beneficial will be more inclined towards InfoSec compliant behaviour [27]. The ethical environment that healthcare professionals operate within would appear to be strong motivator to be InfoSec compliant. Attitude; the ‘psychological contract’; organisational trust and moral judgement, among other elements, combine to form the Attitude construct.

4. Discussion of the Information Security Compliance Model

The complexities in achieving InfoSec compliance illustrate the contention of this research that positive motivators may be more effective in attaining InfoSec compliance. Factors that promote InfoSec compliance are regarded to be powerful motivators while those which deter information misuse have yet to be proven as wholly successful [10,29].

![Fig 2 – Information Security Compliance Model](image)

The ISCM, illustrated in Fig.2, holds that an alteration in the attitude of the users will improve InfoSec compliant behaviour. This, it is proposed, can be achieved by altering the messages provided through the Body of Knowledge. The ISCM is proposed as an instrument to modify the InfoSec compliant behaviour of the users. It comprises various constructs and represents a preliminary version. Its major components are, to recap, as follows:

- The InfoSec compliance promoting and misuse deterrence factors are represented as the Misuse Deterrence and Compliance Promoting constructs;
- The Body of Knowledge construct which comprises the security policies, awareness and education programs;
- Skills construct which combine the computer self-efficacy with other features exhibited by the user;
- Behavioural Intervention construct refers to the use of the CMUA and Appraisal Tendency Framework for Classifying Emotions. It is used to evaluate the Attitude of the user;
• Attitude construct comprises the beliefs, feelings and intention components with other factors;

• Security Complaint Behaviour is the goal achieved through the interaction of the model constructs.

The interaction, direct and indirect, between the constructs is briefly explained, a full description of its operation is beyond the scope of this forum. The Misuse Deterrence and Compliance Promoting factors exert an indirect influence on the Attitude construct. Their main influence is, within the Body of Knowledge, through the originating theory applied to its components. It affects the Skills construct directly through its policies and programs.

Presently, a Misuse Deterrence approach which employs prescriptive and deterrence methods is the main influence evident in the Body of Knowledge. Its components are, in the main, based on the theory of general deterrence using the fear of punishment and sanctions to promote compliance. These methods are patently unsuccessful as demonstrated by the recent survey results of [17].

Compliance Promoting factors change the message contained in the Body of Knowledge to one of positive motivation, through explaining the benefits and positive effects of compliant behaviour. Positive emotions towards behaviour promotes its repetition. InfoSec complaint behaviour is based on the ad hoc decisions of the users; therefore, the attitude of the user is changed from being compliant due to fear of punishment to one of being compliant because the message communicated in the Body of Knowledge is aimed at the user’s sense of achievement and self-efficacy among other outcomes. This will promote a sense of positive attributed trust and is intended to appeal to the strong sense of ethics; moral obligation and judgement; and organizational trust that are profound elements of the healthcare professional environment.

The effect of altering the theoretical basis of the Body of Knowledge is evaluated by the Behavioural Intervention construct. It evaluates which Appraisal Tendency Framework Quadrant has been affected by the change to the Body of Knowledge doctrine. The expected goals include; that the user’s reactions will reflect a more positive attitude towards the InfoSec measures and that a shift towards the Challenge and Achievement Quadrants is affected.

It is known, for example, that healthcare professionals show greater concern for clinical data than personal patient information. A message, communicated through the Body of Knowledge, about the benefits of protecting patient confidentiality will prompt the realisation that maintaining the dignity of the patient, through protecting his privacy at both life and death, is as important as protecting the confidentiality of their tests results.

The protection of patient personal information is stipulated in the Hippocratic Oath and acts as a determinant of the ethical healthcare environment. A shift in InfoSec compliance motivation to one driven by the Challenge and Achievement Quadrants can align the behaviour of the healthcare professional with their inherent moral judgement, need for autonomy and inter-personal trust. The decision to behave ethically through InfoSec compliance rests with the healthcare professional.

An opportunity exists to motivate an alternative approach to InfoSec compliant behaviour, in the face of the dismal performance of the sanction and deterrence focused approaches. This research motivates the use of Compliance Motivating factors as that alternate.

5. Conclusion

It is apparent that the attitude of the user affects Information Security Compliant behaviour. Research, in the main, attempts to prevent user misuse and abuse but there is little research addressing the promotion of compliance. The proposed solution presented in the ISCM attempts to engender InfoSec compliant behavior through the Compliance Promoting factors. These realign the message contained in the Body of Knowledge to one that promotes the benefits of InfoSec compliance. It is anticipated that this research will lead security practitioners to review the over-riding message of deterrence and sanctions presented in policies and procedures in existing Bodies of Knowledge. This is a matter for further research.

Acknowledgements

The financial assistance towards this research, given by the National Research Foundation (NRF), is hereby acknowledged. Opinions expressed, and conclusions arrived at, are those of the authors, and should not be attributed to the NRF.
References


