

## Chapter 54

# Strategic Approach towards Clinical Information Security

**Sangseo Park**

*The University of Melbourne, Australia*

**Jane Moon**

*University of Melbourne, Australia*

### ABSTRACT

*Information security in the health information system has been technology-centric and no strategy has been put forward to meet the demands of the rapid adoption of e-Health in the health industry. The implementation of security requires a good understanding of the stake holders involved and requires the technical aspect of clinical information security, including security requirements, access control and disclosure control. However, since technology-centric security is prone to failure, a stringent strategic approach is quintessential. This chapter discusses the ways to safeguard medical information assets from the strategy point of view. This study shows that most of the existing clinical information security literature and practice has been focused on tactical prevention at a technical level. This understanding of the current status of clinical information security not only suggests the need for a shift from the technical approach to the strategic approach but also raises the necessity for the employment of multiple strategies working in a harmonised way.*

### INTRODUCTION

With the computer becoming ubiquitous and with the increased use of cloud computing for dissemination of health information, there is an increased risk of various types of security threats (El Emam, Neri, & Jonker, 2007; Huston, 2001; Lorence & Churchill, 2005; Mercuri, 2004).

Some of the security threats to healthcare information are: private use by privileged insiders (Anderson, 1996a), illegal use of information by third parties such as social workers and insurance companies (Anderson, 1996a; Kumar & Lee, 2011), unauthorized use of resources (Win, Susilo, & Mu, 2006), unauthorized alteration of resources and information (Win et al., 2006), the loss, release or theft of items of equipment and digitised medical information (Bønes, Hasvold, Henriksen, & Strandenaes, 2007; Clayton

DOI: 10.4018/978-1-5225-2237-9.ch054

et al., 1997), and disclosure at the communication channel between head surgeries/clinics and branch surgeries/clinics and at the devices participating in the communication (Bønes et al., 2007; Kumar & Lee, 2011), the repudiation of actions (Win et al., 2006), the unauthorized denial of service (Kumar & Lee, 2011), and the exposure of mobile healthcare devices to insecure zones (Bønes et al., 2007).

These threats target sensitive information such as fertility and abortions, emotional problems and psychiatric care, sexual behaviours, sexually transmitted diseases, physical abuse problems and genetic predispositions to diseases (Rindfleisch, 1997). Especially, the shift towards digitised and networked healthcare services via the Internet and/or mobile technologies, such as Health Bank (Ramsaroop & Ball, 2000), aggravates security concerns and, as a result, stimulates the development of relevant technologies (Dong & Dulay, 2006; Hung, 2005; Peyton, Hu, Doshi, & Seguin, 2007; Raman, 2007; Zheng, Chen, & Hung, 2007). More importantly, the probability of security breaches in the healthcare sector is steadily on the rise, from 8.14% in 2005 to 30.84% in 2010 (Collins, Sainato, & Khey, 2011).

The existing security measures are insufficient to provide a satisfactory level of protection to clinical information assets (Win et al., 2006) and for protecting genetic privacy (Erllich & Narayanan, 2014). There is a significant gap, regarding awareness of clinical information protection, between healthcare providers and patients. Medical practitioners and institutions are relatively less sensitive than patients regarding the breach of healthcare information (Collmann & Cooper, 2007; Emam, Moreau, & Jonker, 2011; Kruger & Anschutz, 2013; Likourezos et al., 2004; Stahl, Doherty, & Shaw, 2012). They exhibit a similar attitude even to the use of hand-held devices, which are known to be more vulnerable, in clinical practice (McAlearney, Schweikhart, & Medow, 2004). On the other hand, a significant percentage of patients are concerned about the possibility of medical information leakage from health websites that share information without their permission (Raman, 2007). Hence, the protection of clinical information assets is regarded as a major concern requiring long-term and continuing attention in the healthcare industry (Ammenwerth, Buchauer, Bludau, & Haux, 2000; Figg & Kam, 2011; Gritzalis & Lambrinou-dakis, 2004; Kahn & Sheshadri, 2008; Win, 2005).

Information security has traditionally been approached from technological perspectives, because it is hard for information security to be independent of technology. This standpoint is based on the notion that information security is a matter of quality of technology, and that security issues can be easily addressed by applying it (Browne, 1972; Choo, 2011; Hoffman, 1969; Iivari & Hirschheim, 1996). However, a technology-centric approach has a high possibility of failure (Alberts, 2002; Landwehr, 2001; Von Solms, 2000). Current attacks are becoming sophisticated and intelligent (Gandotra, Singhal, & Bedi, 2009; Kewley & Lowry, 2001; Price, 2010; Rosenquist, 2008); Some of them are innovative to the extent of taking advantage of newly found vulnerabilities within a day (Levy, 2004); Some attacks use internal members of an organisation as stepping stones to penetrate existing security barriers of the organisation (Baize, 2012); In addition, there exist attacks originating from inside an organisation, which are hard to recognise and control using current security measures focusing on attacks from outside (Humphreys, 2008; Schultz, 2002; Theoharidou, Kokolakis, Karyda, & Kiountouzis, 2005). On the other hand, information systems cannot be flawless or vulnerability-free (Lampson, 2004; Peterson, 2007; Price, 2010). Furthermore, old vulnerabilities remain within information systems without being completely eliminated (Hayes, Shore, & Miles Jakeman, 2012), and new ones keep being reported (Saydjari, 2004; Wood et al., 2012). In this climate, although some new ways of protecting clinical information have been attempted in genetic testing (Erllich & Narayanan, 2014) and data identification (Benitez & Malin, 2010), these are insufficient, since they focus on certain aspects of protection rather than securing clinical information

29 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:  
[www.igi-global.com/chapter/strategic-approach-towards-clinical-information-security/180633](http://www.igi-global.com/chapter/strategic-approach-towards-clinical-information-security/180633)

## Related Content

---

### Strength from Spirituality

Eric T. Wanner and Jennifer Lynne Bird (2015). *Innovative Collaborative Practice and Reflection in Patient Education* (pp. 237-253).

[www.irma-international.org/chapter/strength-from-spirituality/123632](http://www.irma-international.org/chapter/strength-from-spirituality/123632)

### Clinical Educator Track Resident Programs: Lessons Learned From Innovative Programs

Michael W. Stumpf and Sonya D. Hayes (2020). *Handbook of Research on the Efficacy of Training Programs and Systems in Medical Education* (pp. 327-344).

[www.irma-international.org/chapter/clinical-educator-track-resident-programs/246636](http://www.irma-international.org/chapter/clinical-educator-track-resident-programs/246636)

### A Longitudinal Study of Facilitating Medical Students' Stepwise Transformation to Distance Learners

Fanny Pettersson and Anders D. Olofsson (2015). *Transformative Curriculum Design in Health Sciences Education* (pp. 235-274).

[www.irma-international.org/chapter/a-longitudinal-study-of-facilitating-medical-students-stepwise-transformation-to-distance-learners/129434](http://www.irma-international.org/chapter/a-longitudinal-study-of-facilitating-medical-students-stepwise-transformation-to-distance-learners/129434)

### Privacy-Friendly Management of Electronic Health Records in the eHealth Context

Milica Milutinovic and Bart De Decker (2017). *Healthcare Ethics and Training: Concepts, Methodologies, Tools, and Applications* (pp. 528-542).

[www.irma-international.org/chapter/privacy-friendly-management-of-electronic-health-records-in-the-ehealth-context/180600](http://www.irma-international.org/chapter/privacy-friendly-management-of-electronic-health-records-in-the-ehealth-context/180600)

### Understanding Your Learner: Conducting a Learner Analysis

Tina M. Souders (2017). *Advancing Medical Education Through Strategic Instructional Design* (pp. 1-29).

[www.irma-international.org/chapter/understanding-your-learner/174222](http://www.irma-international.org/chapter/understanding-your-learner/174222)