Received 31 August 2017
Revised 27 November 2017
Accepted 3 January 2018

Reconciling value-based objectives for security and identity management

Kane J. Smith
Virginia Commonwealth University, Richmond, Virginia, USA
Gurpreet Dhillon
University of North Carolina at Greensboro, Greensboro, North Carolina, USA, and
Karin Hedström
School of Business, Örebro University, Orebro, Sweden

Abstract

Purpose – In this paper, using values of individuals in a Swedish health-care organization, electronic identity management objectives related to security are defined.

Design/methodology/approach – By using value-focused thinking, eliciting values from interviews of three groups of health-care staff's objective hierarchies for three stakeholder groups are identified and defined. Objective hierarchies allow comparison across multiple stakeholder groups such that strategic objectives for identity management can be compared and contrasted.

Findings – This qualitative investigation, which used value-focused thinking, revealed 94 subobjectives, grouped into 12 fundamental and 14 means objectives, which are essential for developing measures that address potential value conflicts in a health-care organization around electronic identity management. The objectives developed in this study are grounded socioorganizationally and provide a way forward in developing measures aimed to reducing potential conflicts at a policy level.

Originality/value – In a final synthesis, congruence (or lack thereof) in the electronic identity management approach for a Swedish health organization is suggested. This also creates a foundation to evaluate and weight different objectives for strategic decision management.

Keywords Health care, Identity management, Value-focused thinking

Paper type Research paper

1. Introduction

Advances in use of IT in health care have generated discussions on individual identity. While health-care management strives to deliver services in an efficient and effective manner, patients aspire to maintain identity of their self and their electronic records. In an ideal situation, there should be complete congruence between corporate and individual needs. Law demands that patient records are kept confidential. Identity management is often viewed as the solution to guarantee secure access to sensitive patient data, at the same time as visions of efficiency, interoperability and timely access to patient data irrespective of location can be realized (Halperin and Backhouse, 2008). But, considering the very nature of

Information & Computer Security
Vol. 26 No. 2, 2018
pp. 194-212

2056-4961
DOI 10.1108/ICS-08-2017-0059

The research for this paper was financially supported by Swedish Knowledge Foundation and Swedish Civil Contingencies Agencies, who made this research possible. The authors also thank Fredrik Söderström, Linköping University, Sweden, who graciously shared his data with them. Without his support, this paper would not have been written.

federated systems that exist, maintaining security can be a challenge. There is usually a lack of unanimity of purpose between the values propounded by the corporate and the values cherished by the individuals. Consider a situation where there is a need to retrieve pertinent data for a specific treatment for a patient. The situation demands that that patient records are searched and retrieved from several locations based on patient identifying information. To define a treatment plan, extensive use of identity management practices is required. Adequate technology support is essential; there is a need for rule structures relevant to the authorization process. And there is a need for awareness and training of various stakeholders. It is only then that a high integrity electronic identity (eID) management system can be put in place.

In this paper, we identify value conflicts amongst stakeholders involved in the implementation of an electronic health identity management system. Based on the value conflicts, we develop principles that strategic planners need to be cognizant of. The paper is organized as follows. First, we review the latest developments in electronic identity management in the context of health care. Second, based on our assessment of identity management system implementation, we define value-based objectives and develop value model to demonstrate the interactions between means and fundamental objectives. The context of value-based objectives is a Swedish health-care organization composed of three distinct stakeholder groups, namely, operations professionals, IT professionals and medical professionals. Finally, we sketch out principles necessary for reconciling and prioritizing objectives.

2. Electronic identity management in the literature

For health care, the use of electronic identification management is seen an efficient tool for the identification and authentication of individuals when accessing sensitive information such as patient data (Stroetmann *et al.*, 2011). The availability of an identity management solution is considered a necessary "building block" for the delivery of "robust, streamlined and sustainable" public e-services by European governments to their citizens (European Commission, 2010). On an organizational level, has the development from paper-based records in favor of electronic health care records "pushed health care into the lead for identity management application areas" (Halperin and Backhouse, 2008). However, balancing the need for timely access to accurate patient information with the need to safeguard the confidentiality and integrity of that information can create a great deal of tension giving rise to specific challenges for identity management in health care. Halperin and Backhouse (2008) argue that security and privacy is one of the key issues of identity management together with interoperability and questions about convenience and intrusiveness. There are also some challenges that are specifically related to eID within health care. For instance, Campos *et al.* (2011) argued that issues concerning identity management within health care tend to center on interoperability, together with responsibilities and roles. A study carried out by Hedström *et al.* (2016) illustrated how usability, together with users' attitudes behaviors and privacy concerns are important challenges in relation to the implementation of eID within health care.

3. The use of value-based objectives in the literature

The practice of incorporating public values into the policy-making decision process has a robust basis in the academic literature, where the public's opinion is intended to drive policy creation and implementation (Dhillon and Smith, 2017; Dhillon *et al.*, 2016; Dhillon and Torkzadeh, 2006; Drevin *et al.*, 2007; Keeney, 1994, 2006, 2013; Keeney and Palley, 2013; May *et al.*, 2013; Merrick and Garcia, 2004; Merrick *et al.*, 2005a; Merrick *et al.*, 2005b;

Witesman and Walters, 2014). The opinion of the public is driven by the inherent values of the collective individuals and is very useful for creating policy that is both effective and accepted by those affected through its implementation (Keeney, 1999, 2006; Dhillon *et al.*, 2016; Dhillon and Torkzadeh, 2006). Due to the aforementioned benefits, public values are an important consideration within policy decisions and should be incorporated into the decision-making process, despite being a difficult task (Dhillon *et al.*, 2016; Dhillon and Torkzadeh, 2006; Keeney, 1999, 2006; Witesman and Walters, 2014). The uses for all forms of patient-centric data in health care is growing rapidly, giving rise to new privacy and security concerns for those about whom the data are being collected. Current policies do not adequately account for these concerns and so it cannot adequately address privacy and security concerns in this.

4. Methodology for defining value-based objectives

According to Keeney (1999), to identify values one must ask the concerned people, meaning anyone that can be considered as having a stake in solving the problem at hand. Within the academic literature, there is a significant amount of variance in the number of individuals that should be interviewed in the process. As an example, Hunter (1997) used the interviews of 53 people from two different organizations to do a content analysis to elicit individual values. However, Phythian and King (1992) used two managers who were experts in assessing tender enquiries to identify key factors and rules that influence tender decisions. Additionally, Keeney (1999) obtained interviews from over 100 individuals to obtain their values and develop value-based objectives that influenced their Internet purchases. However, with respect to Keeney (1999) it is important to understand that interviews should continue till saturation of values occurs, which is facilitated naturally within the value-focused thinking approach. For this study, 16 people from three distinct stakeholder groups in the health care field, namely, medical professionals, IT professionals and operations professionals, were interviewed about their experiences of implementation and use of electronic identity management in their organization. We elicited individuals from one hospital ward and two health care centers to obtain a rich understanding of electronic identity management within the three unique stakeholder contexts. The participants were selected as they were highly knowledgeable and had different roles and worked at different sites. This was important as we wanted to uncover and compare different perspectives (Eisenhardt and Graebner, 2007). We complemented our first round of interview using the snowball strategy to make sure we covered the most important and interesting roles (Biernacki and Waldorf, 1981). We asked our informants questions about their view of electronic identity management, how identity management was enacted in practice, i.e. how they used it, how they perceived the implementation of electronic identity management at their work site, functionality and consequences of using electronic identity management. Through their responses we could identify general values for electronic identity management related to information security. The interviews were classified into 124 value responses. This allowed us to cluster these common form value statements into 94 subobjectives which were then able to be grouped into 12 fundamental and 14 means objectives. The following is an explanation of the process used through which these fundamental and means objectives were obtained for our research.

The following three-step process (See Figure 1) is used to identify and organize the values that an individual might have with respect to electronic identity management for ensuring patient privacy in health care (Keeney, 1992): First, interviews are conducted which elicit the values an individual might have within a decision context. Second, individual values and statements are converted into a common value format, such as an objective oriented

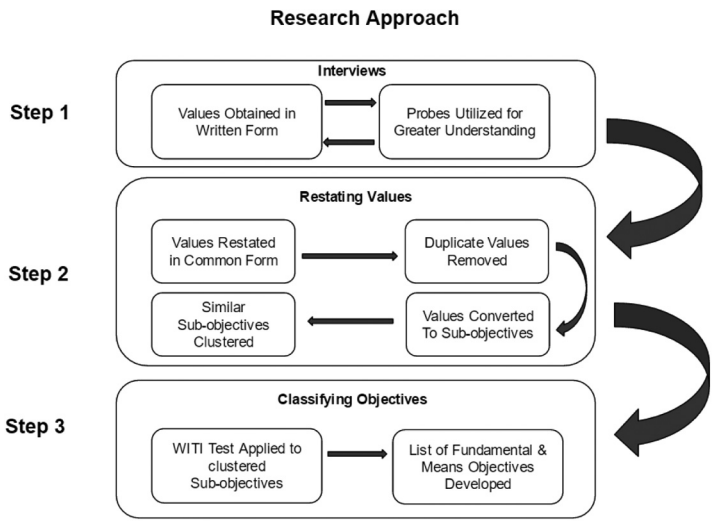

Figure 1.
The research approach

statement. Then similar objectives are grouped together to form clusters of objectives. Finally, the objectives are then classified as either fundamental to the decision context, resulting in a fundamental objective or simply a means to achieve the fundamental objectives, which is known as a means objective.

4.1 Identifying values

To begin, interviews are conducted with the concerned peoples as a process of identifying values. We at the beginning of each interview, the purpose is clarified and context and scope of the interview are established. The core objective in this interview is to understand the implementation and use of identity management in health care. All questions were open-ended. As individuals can express values differently, an inherent difficulty exists with the quiescent nature of the values, so different probing techniques are used to identify latent values. Keeney (1992), as probing techniques, suggests words like trade-offs or consequences as useful in making such implicit values explicit.

4.2 Structuring values

Once the values are identified, a process of value structuring and objective development begins. Step 1 is that all statements are restated in a common form where duplicates are removed. Then, common form values are considered from these statements and converted into subobjectives. According to Keeney (1999), an objective is constituted of the decision context, an object and a direction of preferences, which in the case of this research is electronic identity management in health care. With all values systematically reviewed and converted into subobjectives, it may be found that a number of subobjectives deal with similar issues, making it necessary to determine if these overlapping clusters should be merged or stand alone. By carefully reviewing the content of each of these subobjectives, clusters are developed that group similar ones together (thus removing any overlap) and then each cluster of subobjectives is labeled by its overall theme which then becomes the main objective of the cluster.

4.3 Organizing objectives

The list of subobjectives and corresponding clusters initially include both means and fundamental objectives so we must differentiate the two. This is accomplished by repeatedly linking objectives through means–ends relationships then specifying the fundamental objectives. To identify fundamental objectives, the question is asked, "Why is this objective important in the decision context? (Keeney, 1994)". If the objective is an essential reason for interest in the decision context, then the objective is a candidate as a fundamental objective. If the objective is important due its implications with respect to some other objective, then it is a candidate as a means objective. This is termed by Keeney (1994) as the "WITI test". In our research, this test was applied to each stakeholder group's values to create three sets of fundamental and means objectives.

5. Objectives for understanding electronic identity management in health care

In this section, we present the fundamental (Table I) and means objectives (Table II) and how they can collectively contribute to facilitating patient privacy through the use of electronic identity management in the form of a network diagram (Figure 2/3/4). In our research we found twenty-six total objectives: 12 fundamental objectives and fourteen means objectives, which are placed into three distinct groups representing the involved

Table I. Fundamental objectives

Operations professionals	Health-care professionals	IT professionals
F1 Ensure confidentiality of patient data	F1 Ensure responsibility for patient privacy	F1 Ensure confidentiality of patient data
F2 Ensure compliance with organizational rules	F2 Ensure confidentiality of patient data	F2 Ensure availability of patient data
F3 Maximize efficiency of organizational procedures for patient privacy	F3 Ensure efficient information flow for patient treatment success	F3 Ensure ease of access to patient data for authorized users
F4 Maximize care delivery through effective information use	F4 Ensure stability in information technology use	F4 Ensure integrity of patient data is not compromised

Table II. Means objectives

Operations professionals	Health-care professionals	IT professionals
M1 Ensure use of authentication tools by medical staff	M1 Ensure responsible access to patient data during house calls	M1 Ensure use of electronic signatures
M2 Maximize organizational competence through training	M2 Ensure efficient identity management	M2 Maximize system uptime
	M3 Maximize token access	M3 Minimize authentication delays
	M4 Maximize fast access to patient data	M4 Ensure external system integration
	M5 Maximize flexible work processes	M5 Ensure internal system integration
M3 Ensure clearly defined data handling procedures		
M4 Ensure availability of patient data for medical professionals' use		

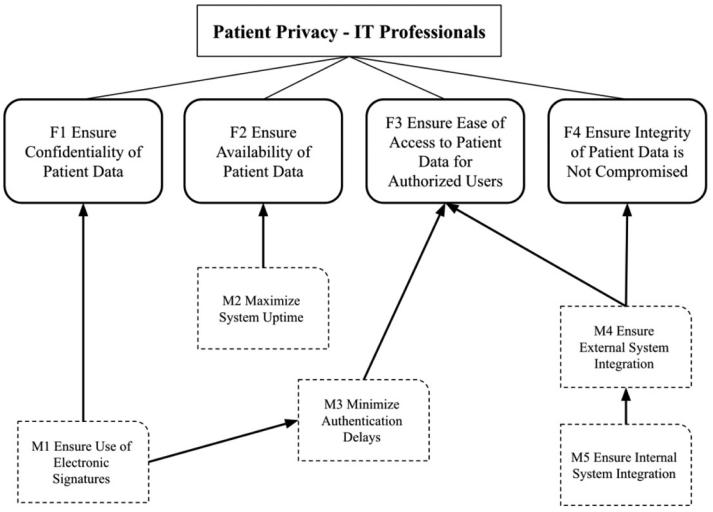

Figure 2.
Means-end network diagram – IT professionals

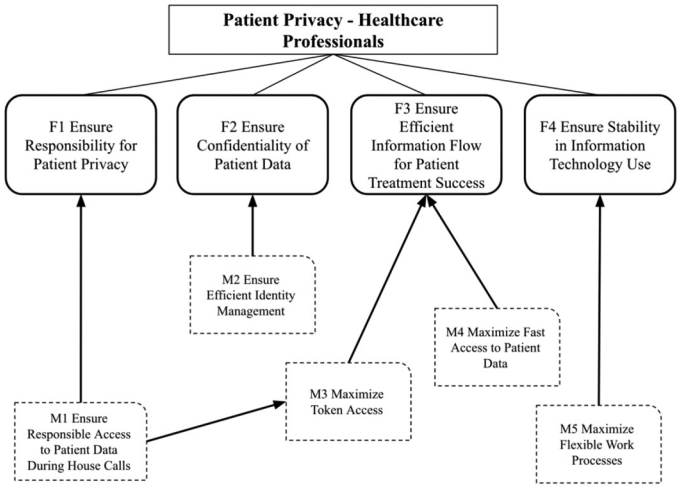

Figure 3.
Means-end network diagram – health professionals

stakeholder groups. The fundamental and means objectives build the means-end network model which can act as a decision pathway to model different decision context for achieving the fundamental objectives. They also present additional research opportunities for modeling dependent and independent variables using techniques, such as structured equation modeling, to determine the effect these moderating means objectives have on the fundamental objectives. Further, multi-criteria decision analysis techniques can be used to construct decision models for evaluating decision context with multiple alternatives based on the concept of maximum expected utility for a given solution.

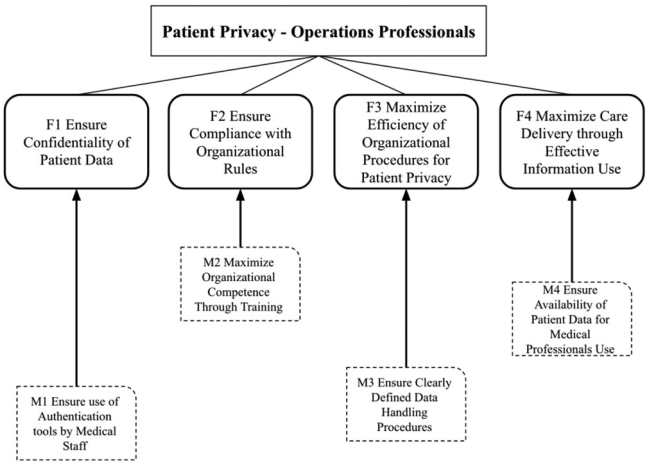

Figure 4.
Means-end network diagram – operations professionals

5.1 Fundamental objectives

The 12 fundamental objectives are divided into three distinct groups, namely, operations professionals, IT professionals and health professionals. The purpose of this research was to explicate the stakeholder values for each group, demonstrating the objectives which they believe to be fundamental to the decision context. It is important to note that some overlap may exist between the objectives intent for each stakeholder group. However, the means by which these groups believe the fundamental objective should be achieved may vary, hence the importance the means-end network diagram. The following are explanation of the fundamental objectives providing an explanation and link to the literature when appropriate as well as a value quote that demonstrates the foundation from which the objective was developed.

5.1.1 Operations professionals fundamental objectives.

5.1.1.1 FO1 ensure confidentiality of patient data. The confidentiality of patient data appears organizationally important, regardless of stakeholder group as they all stated the need to protect the privacy of patient information. However, each stakeholder group viewed confidentiality differently as, for example, those in the operational stakeholder group believed that enforcing the use of authentication tools would improve patient security and reduce the risk of unnecessary or improper access to patient data by unauthorized users. A study by Neeraj *et al.* (2014) support this belief as they conducted a study within a health-care organization and assessed access controls to 59 terminals with access to sensitive patient data. Neeraj *et al.* (2014) found that over 85 per cent of the terminal could be accessed with generic username and password credentials, providing a clear dangerous to the protection of patient data. The proposed remedy by the health-care organization interviewed for our research, authentication tools like login tokens, would eliminate such a threat to patient privacy and is a common tool in electronic identity management. This is supported by the following value quote from the operations professional: "This is a way to guarantee secure authentication".

5.1.1.2 FO2 ensure compliance with organizational rules. When tasked with facilitating patient privacy through the use of electronic identity management, operations professionals clearly emphasized the need for compliance with organizational rules. While a policy may be developed that is comprehensive in nature so as to cover all necessary aspects of patient

privacy, if an employee fails to comply with said policy then it has all been for nothing. This is supported by value statements such as "Several users use workarounds to access the system, instead of using the card". Additionally, the academic literature supports the conclusion that compliance failures by employees represent a threat to organizations as well (Chen *et al.*, 2012). A study by Chen *et al.* (2012) found that mechanisms for ensuring compliance like punishments did not work and that training programmes that rewarded desired behaviors were more effective. This amply supports the desire by operations professionals to train expected compliance behaviors to ensure patient privacy is maintained by the organization.

5.1.1.3 FO3 maximize efficiency of organizational procedures for patient privacy. In this organizational context, operations professionals are seeking efficiency in the procedures for ensuring data privacy in health care. In the face of constraints on their resources, decision-makers must set practical expectations to facilitate organizational success (Gibson *et al.*, 2004). This means that organizations should set priorities regarding process criteria, elements and parameters for success to ensure critical needs are met, while eliminating unnecessary burden (Gibson *et al.*, 2004). This is supported by value statements such as "The procedure to log in had been made simpler and more efficient. Now we only log-in using the card".

5.1.1.4 FO4 maximize care delivery through effective information use. Academic research strongly suggests that failures in the coordination of care are common and can create serious quality concerns as information is not being used effectively at the multiple points of patient contact (Bodenheimer, 2008). For example, if patient is hospitalized, their primary care physicians may not be notified when they are discharges, and summaries of their discharge may not contain sufficient information or never even reach the primary care practice (Bodenheimer, 2008). This speaks to the importance of effective information use by health care. Operations professionals expressed the strong desire for electronic identity management to facilitate such effective information transfer by allowing medical professionals to quickly and easily transfer confidential patient information in a secure manner between authorized medical professionals, as well as between different sites: "It is easy to move between different work sites. The physicians move around quite a lot".

5.1.2 Health-care professionals fundamental objectives.

5.1.2.1 FO1 ensure responsibility for patient privacy. When interviewing health-care professionals, they clearly indicated that it was very important to understand responsibility structures around ensuring patient privacy. Based on their responses it was clear they were expressing the desire to have clear structures of responsibility that delineate the role each professional should play in maintaining patient privacy while delivering care to their patients. This is supported by value statements such as "The identity card is an extra safety feature guaranteeing that it is me who change the medication, or reading the medical record". The academic literature supports this concern as, for example, Barrows and Clayton (1996) point out that a lack of a cohesive security policy that clearly defines roles and responsibilities leads to informational security failures. Therefore, it is important for medical professionals to clearly understand their roles and responsibilities in maintaining patient privacy and how to effectively use tools such as electronic identity management to do so.

5.1.2.2 FO2 ensure confidentiality of patient data. From the health-care professional perspective, the confidentiality of patient data is important, however they clearly advocated for efficient identity management, viewing difficult to use login mechanisms as an impediment to their work. With this understanding, Neeraj *et al.* (2014) support the idea that medical professionals clearly desire protections for patient privacy but need easy access to

such data, potentially leaving patient data vulnerable. Neeraj *et al.* (2014) found that 55 per cent of computers used by medical professionals had easily accessible patient data available on the desktop. While protecting patient data is clearly important to medical professionals, the desire to save patient lives may lead to practices that could compromise patient privacy. Medical staff stress the importance for technical implementations as a support for ensuring privacy. This is supported by the following quote from a medical professional:

> We need these barriers to increase security, because this is not something we understand. It doesn't matter how much we stress it, people still have computers on with medical records on display.

5.1.2.3 FO3 ensure efficient information flow for patient treatment success. For medical professionals, in our study, a clear value was that efficient information flow was critical for patient quality of care and therefore essential. To this end, they expressed the desire for technology to facilitate efficient transfers of information between authorized professionals to improve patient care or the possibility for medical staff to work from several sites. This is supported by the following quote from a medical professional: "It now works better to access the information when you change computers - you can bring with you the information you already opened". This desire is supported in the literature as, for example, Devaraj *et al.* (2013) found that streamlining patient information flow in health-care organizations resulted in a significant improvement in overall patient quality of care.

5.1.2.4 FO4 ensure stability in IT use. The integration of new health care technology can provide a competitive advantage to an organization, improving quality of care, streamlining processes and reducing costs (Angst and Queenan, 2011). However, health-care professionals in our study noted that stability in the technology used to protect patient privacy should be stable, not requiring medical professionals to continuously learn new systems and integrate new technologies into their work processes. While the academic literature demonstrates that integrating new technology in health care can lead to overall improvements in quality of care (Angst and Queenan, 2011), health-care professionals clearly desire a level of stability with respect to technology. This is supported by the following quote from a medical professional:

> Previously we needed to use several log-ins. It was technical issues that affected our view of the identification system. It was more troubling, than helping. Yet another thing to do.

5.1.3 Information technology professional's fundamental objectives.

5.1.3.1 FO1 ensure confidentiality of patient data. The IT professional stakeholder group provides a unique perspective when dealing with the confidentiality of patient data. While health-care professionals and operations professionals also view patient privacy as important, IT professionals appear to approach it by attempting to assign responsibility or attribution for information confidentiality to the user. For example, a value quote by an IT professional, "This is for secure authentication" indicates that attribution of responsibility via electronic methods would help to ensure the confidentiality of patient data. For example, Neeraj *et al.* (2014) found that only 26 per cent of computers accessed by medical staff were free of confidential patient data and that 85 per cent of computers had been logged in to using generic credentials. This presents a problem when attributing violations to a particular user and speaks to the clear desire by IT professionals to have a means finding users who violate protocols.

5.1.3.2 FO2 ensure availability of patient data. Within the group of IT professionals interviewed, there is a clear understanding that having access to quality patient data by medical professionals can lead to improved patient care outcomes. However, despite the

enormous expenditure aimed at improving patient outcomes by health-care systems, clinical outcomes remain suboptimal (Belle *et al.*, 2015). A key factor attributed to such inefficiency in spend-to-outcome is the inability to effectively gather, share and use information in a more comprehensive manner within the health-care systems (Belle *et al.*, 2015). Clearly, IT professionals recognize then that medical professionals need access to patient data to drive positive outcomes and then any electronic identity management system should facilitate 24/7 availability of patient data. But there is also a risk related to this. For example, a value quote by an IT professional, "But there is a risk that you can't access the information if the technology falters", supports this understanding.

5.1.3.3 FO3 ensure ease of access to patient data for authorized users. In the same vein as availability of patient data to drive clinical outcome success by medical professionals (Belle *et al.*, 2015), IT professionals also state that ease of access is critical for authorized users while still maintaining patient privacy. It can be said that even if the data exists and is available to the medical professionals, if they are unable to access the data quickly and easily, then it still hinders the medical process. Additionally, academic literature such as Li *et al.* (2010), advocate that patient privacy can be easily maintained by using authentication and encryption controls unique to the user. By keeping controls simple and unique to the user, potential violations would be easy to trace and controls and encryption in place, avoiding generic login credentials to ensure ease of access. In the case of identity management using electronic identity cards, this is related to how you handle your card. This is supported by the following value quote from an IT professional: "We don't want people to share their cards".

5.1.3.4 FO4 ensure integrity of patient data is not compromised. IT professionals recognize that ensuring the integrity of patient data is critical for ensuring successful patient outcomes. One important factor in this is to have technical solutions that work together. This is supported by the following value quote from an IT professional: "There are many technical solutions that need to harmonize". It is important to recognize that the integrity of patient data represents the basis for clinical decisions made by medical professionals and that if it is compromised it can lead to poor outcomes. For example, a study by Pothier *et al.* (2005) found that when data were cycled through a manual medium, by the third cycle the integrity of the data had completely deteriorated. When data were moved to hard recordings, data loss was minimal, however if data related to patient care is not cycled into the system quickly and efficiently, the integrity of the data is quickly compromised and can be called into question. Therefore, based on this understanding, IT professionals have clearly expressed that the integrity of the data is fundamental when considering electronic identity management and must not inhibit data transfer into an electronic medium (i.e. electronic medical record).

5.2 Means objectives

The 14 means objectives are also divided into three distinct groups, namely, operations professionals, IT professionals and health professionals. As the purpose of this research was to explicate the stakeholder values for each group, demonstrating the objectives which they believe to be fundamental to the decision context, the means by which those fundamental objectives should be achieved are also important to consider. Additionally, some overlap may exist between the objectives intent for each stakeholder group, just as they did for the fundamental objectives. However, the means by which these groups believe the fundamental objective should be achieved do vary, hence the importance the means-end network diagram in illustrating the differences and similarities. The following are

explanation of the means objectives providing an explanation and a link to the literature when appropriate that demonstrates the basis of support for the objective being described.

5.2.1 Operations professionals means objectives.

5.2.1.1 MO1 ensure use of authentication tools by medical staff. Operations professionals recognize that certain tools used by medical staff for authentication can represent both positive and negative consequences, however research bears out that the benefits can outweigh the negatives. For example, Khan and Kumari (2014) found that smart cards could be susceptible to login credential theft and therefore compromise patient data, if medical staff were to lose a card and it fell into the wrong hands. However, Khan and Kumari (2014) presented a novel method for ensuring the susceptibility of data loss due to the theft or loss of authentication tools could be minimized using wireless medical sensor networks in conjunction with authentication tools like login tokens and badges. This supports the value held by operations professionals that authentication tool technology is necessary and its use should be enforced to enable better security of patient data while minimizing workflow impacts.

5.2.1.2 MO2 maximize organizational competence through training. The academic literature bears out that security can come from organizational competence via human capital and that a good way to achieve such competence to this point is through training (Furnell *et al.*, 1997). This supports the values espoused by operations professionals that the best means of achieving organizational competence if to enhance employee training programmes. The belief is such that if employees understand the ways in which they should handle patient privacy, they will be more likely to do so. This includes, as supported by the literature, the use of things such as ways in which relevant information may be disseminated to staff, including security guidelines, training seminars and World Wide Web-based services (Furnell *et al.*, 1997).

5.2.1.3 MO3 ensure clearly defined data handling procedures. Clearly defined data handling procedures can result in superior organizational culture as it can create a responsible and consistent reporting structure (Hutchinson *et al.*, 2009). It can be said that operations professionals intuitively understand this concept and have therefore advocated for clearly defined data handling and reporting procedures. Organizational culture where procedures and clear and consistent will therefore result in safer culture and patient privacy will be more likely be protected (Hutchinson *et al.*, 2009).

5.2.1.4 MO4 ensure availability of patient data for medical professionals' use. The use of data in health care has evolved into an essential tool for providing valuable insights into patient care, treatments and ultimately improving outcomes while reducing organizational costs in the delivery of care (Raghupathi and Raghupathi, 2014). Therefore, operations professionals in this study clearly believe that due to the organizational value provided by such use of data, that medical professionals need maximum availability for use in treating patients.

5.2.3 Health-care professionals' means objectives.

5.2.3.1 MO1 ensure responsible access to patient data during house calls. Medical professionals that participated in our study made it clear that having access to patient data during house calls was a means by which they believed data availability could be improved. Having access to patient records on location in a secure manner via electronic methods would protect patient privacy, yet allow them to make better decisions, being able to access more information more quickly. However, numerous legal and ethical implications exist which must be addressed as medical professionals must keep patient information confidential, taking precautions to preserve patient information (like electronic identity management), trust and the integrity of the patient–physician relationship (Spielberg, 1998).

5.2.3.2 MO2 ensure efficient identity management. During our study, medical professionals pointed out that as a means of protecting patient information, identity management must be an efficient process. Any process that conflicts with their ability to provide patient care would be viewed negatively and detrimental and therefore any technology must be efficient. While it is clear based on the literature that technology improves efficiency, the manner in which medical professionals in our study want it delivered is rather specific (Chaudhry *et al.*, 2006). Medical professionals require efficient mechanisms for managing identity, which they believe will result in patient data confidentiality being maintained.

5.2.3.3 MO3 maximize token access. With respect to electronic identity management, medical professionals believed that having this kind of tool should allow them to maximize their access to patient data for their specific needs. This is taken as, maximize their access to information that they need to treat a patient, but minimize access to superfluous information that is unnecessary and may compromise patient privacy. This value was expressed by numerous medical professionals in our study, believing this a clear means of maximizing the benefits of electronic identity management in their organization.

5.2.3.4 MO4 maximize fast access to patient data. To deliver the best care, they feel possible, medical professionals in our study indicated they needed quick access to relevant patient data to ensure their decisions were well informed. They believe that electronic identity management controls should facilitate fast access to the necessary patient data base on the medical professionals needs. Therefore, this objective is viewed by medical professionals as a means to fulfilling the fundamental objective of ensuring information flow to facilitate treatment success.

5.2.3.5 MO5 maximize flexible work processes. Health care can be viewed as a complex sociotechnical system that involves multiple stakeholders with different goals, including complex evolving technologies, processes and external forces (Holden *et al.*, 2013). For this reason, medical professionals indicated that they value flexible work processes and a means of achieving stability in technology use. As technology continually evolves, having flexibility in work processes to incorporate technology aimed at patient privacy in a manner that benefits the context of the situation is important. The academic literature indicates that is important that human factors are given adequate attention when dealing with system interactions involving evolving technology (Holden *et al.*, 2013).

5.2.4 IT professionals means objectives.

5.2.4.1 MO1 ensure use of electronic signatures. IT professionals interviewed in our study indicated that as a means of ensuring the confidentiality of patient data, they believed the use of electronic signatures would be an appropriate tool. The academic literature bears out that the use of electronic signatures is an essential tool in the context of managing electronic patient records (Bradner *et al.*, 2002). Research further states that the use of the electronic signature must be incorporated in both personnel workflow and document management systems to maximize user acceptance (Brandner *et al.*, 2002).

5.2.4.2 MO2 maximize system uptime. Maximizing system uptime is critical as a means for ensuring availability of patient data. A study by Nelson (2007) found that as computers become embedded in clinical workflow processes, disruptions to access can have serious consequences. Nelson (2007) found that uptime of mission-critical clinical applications is an important marker for those who depend on that data to make decisions as well as those who monitor the operational and financial impact of systems. Hence, IT professionals in our study are well justified in the academic literature, advocating for maximizing system uptime for ensuring the availability of patient data.

5.2.4.3 MO3 minimize authentication delays. As authentication schemes become more complex, such as using biometric authentication tokens, the requirement of large quantities of sensor data and identify verification can be computationally intensive (Koved and Zhang, 2014). The large amount of information to be processed can result in long latencies from the time of the authentication request until the authorization is granted (Koved and Zhang, 2014). This can be worse when there is congestion in the system due to excessive authentication requests, such as at the start of the business day or shift change and interruptions can impact the user's short term memory, slow down task performance, as well as result in user dissatisfaction with the authentication system (Koved and Zhang, 2014). For this reason, IT professionals recognize that it is important that as a means of ensuring access to patient data while maintaining patient privacy, authentication delays must be minimized.

5.2.4.4 MO4 ensure external system integration. Systems integration, from the perspective of IT professionals interviewed in our study, was meant convey the idea that seamless information exchange must occur between various entities involved in a patient's care (i.e. independent primary care physician, hospital specialists, independent imaging centers and emergency room). The literature supports this belief as, for example, a study by Chang *et al.* (2007) found that the success of patient care depends on the aggregation and seamless exchange of information within and across organizational borders, which can be facilitated by various electronic identity management techniques (i.e. via the use of electronic signatures).

5.2.4.5 MO5 ensure internal system integration. Similar to IT professionals' beliefs that external systems integration is important, their health system uses numerous systems that capture, store or facilitate patient data in some capacity. While possessing greater control over internal systems, IT professionals in our study felt this was a necessary means by which the integrity of patient data can be maintained. As health systems continue to transform to models of e-health care, systems integration will continue to be important (Chang *et al.*, 2007).

6. Means-end network diagram

After identifying both the fundamental and means objectives for each group, a means-end network diagram (Figure 2/3/4) is created to illustrate their interaction with each other ("F1" means fundamental objective one, and "M1" relates to means objective one). The purpose of a network diagram is to demonstrate the flow of means objectives into the fundamental objectives, which they help accomplish. Fundamental objectives, as previously stated, are essential to the decision context of electronic identity management in health care, so they are listed to the top of the diagram and at the end of the network's flow. The means objectives are important to the decision context in itself but as a way to achieving some other objective. This is demonstrated by (Figure 2/3/4) linking the means objectives that contribute to another objective and ultimately are necessary for the fundamental objective to be achieved. Some means objectives are necessary or impact fundamental objectives directly, while others appear to impact other means objectives that then serve to impact a fundamental objective. It is important to note the interplay between means objectives themselves as well as fundamental objectives so that as research progresses in this domain, all aspects that influence the fundamental objectives are understood and given adequate consideration.

As the means and fundamental objectives developed by this research are grounded in affected stakeholder's values, it provides a better opportunity for an organization or government to understand the social and technical complexities related to conflicting values from their perspective. In other words, because objectives form the basis for any policy

planning exercise, an organization or government should view our framework as a guiding point for defining their own policy planning efforts with respect to electronic identity management. A well-defined path aimed at managing value conflicts would then not only help in the strategic creation of a comprehensive and effective policy but also help in identifying alternatives to achieve its core purpose (as suggested by Keeney, 1992). In short, the relationships between the means and the fundamental objectives would then help in sketching the paths of policy change to best achieve the goal by providing valuable insight into the decision context.

According to Keeney (1992), the means – ends objectives network is a value model representing both quantitative and qualitative relationships. The purpose of such a model, like most models, is to gain insight into a complex situation and thereby complement intuitive thinking (Keeney, 1992; Power and Sharda, 2007). The best way to describe the utility of the value model is to consider the various fundamental objectives as being O1, [. . .] On and m1 (subobjective) as a fundamental measure for a fundamental objective O1. It follows therefore that the vector m= (m1, m2, [. . .], mn) would provide a description of a particular path in the diagram in which a fundamental objective is delivered. The accumulative value of m would then serve as a measure (quantitative or qualitative) of the idiosyncratic resources and abilities that would fit the decision context (i.e. managing value conflicts in EIM). The best way of illustrating this point is to provide a contextual example that demonstrates the functionality of such a model. To this point, the following is a possible means of using the network diagram to facilitate the creation of useful and strategic electronic identity management policy.

If an organization was looking to ensure confidentiality of patient data (fundamental objective) as a way to facilitate patient privacy in health care, labeled as O1, one input could be to ensure use of authentication tools (means objective) labeled as m1; however, this can have multiple forms as each stakeholder group identified these fundamental objectives, yet different means of achieving it, labeled as m2 and m3. This type of model (Figure 2/3/4) illustrates a decision pathway that is therefore useful in helping health-care organizations in achieving one or all of the fundamental objectives. Additionally, it provides different decision pathways for health-care organizations to achieve the fundamental objective, which then allows them to choose pathways that complement their strengths. Hence, based on the preferred value proposition, a number can then be assigned to the vector m. Therefore, a common value model can be used to represent the utility of these decision pathways and will take the form shown in equation (1) (Keeney, 1992; Akkermans and Van Helden, 2002) where k*i* is the weight ascribed to the objective O*i* and v*i* is the relative desirability scaling:

$$V = m_1 m_{2,\ldots,} m_n = \sum_{i=1}^{n} k_i v_i(m_i) \quad (1)$$

7. Limitations and future directions

Based on the research presented in this paper, there are three broad categories, which exist for future research opportunities. The first opportunity is that the list of objectives identified in this research can be subjected to psychometric analysis using separate large samples. This can help, for example, in developing a model for measuring the effect on patient privacy for health-care organizations implementing policies incorporating electronic identity management tools and policies. A second opportunity exists for intensive research to be undertaken to establish relationships between

particular fundamental and means objectives; however, while Keeney (1992) contends that fundamental and means objectives are related and an implicit, logical relationships appear to exist between the fundamental and means objectives, but specific relationships need to be researched. The final opportunity is such that further quantitative work should be carried out to assess how the subscales of means and fundamental objectives relate to each other.

The findings of this research lay a suitable foundation for developing multidimensional measures to facilitate patient privacy in health care through the use of electronic identity management. For example, Keeney (1999) conducted an extensive study, which interviewed over 100 people to assess their values with respect to Internet commerce. And based on this work, Torkzadeh and Dhillon (2002) were then able to develop instruments, which measured factors that influence Internet commerce success. Much in the same way, the research presented within this paper has established values and objectives that would be a basis for measures evaluating alternative decision pathways for ensuring patient privacy via electronic identity management. Within the is domain, many examples exist of research that involves in-depth qualitative research aimed at the development of theoretical concepts which includes research on organizational consequences of IT (Orlikowski and Robey, 1991), relationship between is design, development and business strategy (Walsham and Waema, 1994) and communication richness (Lee, 1994).

In the cybersecurity field, the topic of electronic identity management to facilitate patient privacy in health-care organizations is constrained by the absence of well-grounded concepts that are developed in a systematic and a methodologically sound manner as the topic itself is still a newer concept. The fundamental and means objectives that are presented in this paper make a contribution towards the development of theory specific to patient privacy through electronic identity management in health care, a largely overlooked is research stream. This research was only the first step to identify means and fundamental objectives as it relates to multiple groups of stakeholder values. The next step in this research is to conduct a quantitative study as was done earlier by Torkzadeh and Dhillon (2002) to come up with an instrument that measures fundamental objectives as it relates to patient privacy in health care as there is a need to develop theory that is specific (Benbasat, 2001).

As with most qualitative research, this study is subject to some limitations. The process of identifying values from interview data is largely subjective and interpretive and while as researchers we maintain a professional distance, there is always a possibility that some of our own biases may influence the results; however, we were conscious of this during all three phases. The previous basis for this research and the critical reflections of the interviewee's statements was useful in helping us show how these various interpretations emerged in the research (Klein and Myers, 1999). For this reason, it is believed that being aware of the intellectual biases actually helped us to be objective within our analysis of the data. Further, Walsham (1995) recognized this to be an issue when carrying out intensive research and in regard to the role of the researcher wrote, "the choice should be consciously made by the researcher dependent on the assessment of [. . .] merits and demerits in each particular case (p. 5)". It is our goal that in strictly following the value-focused thinking method and being conscious that our interpretations should not serve to influence our research, it can provide confidence in the outcome of this study.

8. Conclusion

This paper introduces Keeney's (1999) Value-focused thinking to explore identity management in the health care context, demonstrating that value conflicts exist. By exploring three differing stakeholders within the Swedish health care context, the research presented in this paper illustrates how value conflicts can arise when health information systems are introduced. Such conflicts can lead to tensions between information availability and confidentiality (Mommens, 1999) or between efficiency and confidentiality (Hedström *et al.*, 2011). Hence, the research presented in this paper examines the relatively unexplored area of value conflicts related to electronic identity management in health care. It does so in an attempt to discover the objectives necessary to begin a focused attempt at creating policy aimed at facilitating patient privacy through the use of electronic identity management in health care. This qualitative investigation, which used value-focused thinking, revealed 94 subobjectives, grouped into 12 fundamental and 14 means objectives, which are essential for developing measures that address potential value conflicts in a health-care organization around electronic identity management. The objectives developed in this study are grounded socioorganizationally and provide a way forward in developing measures aimed to reducing potential conflicts at a policy level. Therefore, this is a significant contribution as previous research in this area is underdeveloped and as such falls short of being able to propose tangible measures for understanding and addressing these issues. This research provides a path forward towards developing these measures for organizations and governmental bodies who need to develop effective and efficient policy with limited time and resources.

References

Akkermans, H. and Van Helden, K. (2002), "Vicious and virtuous cycles in ERP implementation: a case study of interrelations between critical success factors", *European Journal of Information Systems*, Vol. 11 No. 1, pp. 35-46.

Barrows, R.C. Jr and Clayton, P.D. (1996), "Privacy, confidentiality: and electronic medical records", *Journal of the American Medical Informatics Association*, Vol. 3 No. 2, pp. 139-148.

Belle, A., Thiagarajan, R., Soroushmehr, S.M., Navidi, F., Beard, D.A. and Najarian, K. (2015), "Big data analytics in healthcare", *BioMed Research International*, p. 16.

Benbasat, I. (2001), "Editorial note", *Information Systems Research*, Vol. 12 No. 4, pp. 3-4.

Biernacki, P. and Waldorf, D. (1981), "Snowball sampling: problems and techniques of chain referral sampling", *Sociological Methods & Research*, Vol. 10 No. 2, pp. 141-163.

Bodenheimer, T. (2008), "Coordinating care - a perilous journey through the health care system", *New England Journal of Medicine*, Vol. 358 No. 10, pp. 1064-1071.

Brandner, R., Van der Haak, M., Hartmann, M., Haux, R. and Schmucker, P. (2002), "Electronic signature of medical documents–integration and evaluation of a public key infrastructure in hospitals", *Methods of Information in Medicine*, Vol. 41 No. 4, pp. 321-330.

Chang, I.C., Hwang, H.G., Hung, M.C., Lin, M.H. and Yen, D.C. (2007), "Factors affecting the adoption of electronic signature: executives' perspective of hospital information department", *Decision Support Systems*, Vol. 44 No. 1, pp. 350-359.

Chaudhry, B., Wang, J., Wu, S., Maglione, M., Mojica, W., Roth, E. and Shekelle, P.G. (2006), "Systematic review: impact of health information technology on quality, efficiency, and costs of medical care", *Annals of Internal Medicine*, Vol. 144 No. 10, pp. 742-752.

Chen, Y., Ramamurthy, K. and Wen, K. (2012), "Organizations information security policy compliance: stick or carrot approach?", *Journal of Management Information Systems*, Vol. 29 No. 3, pp. 157-188.

Devaraj, S., Ow, T.T. and Kohli, R. (2013), "Examining the impact of information technology and patient flow on healthcare performance: a theory of swift and even flow (TSEF) perspective", *Journal of Operations Management*, Vol. 31 No. 4, pp. 181-192.

Dhillon, G. and Smith, K.J. (2017), "Defining objectives for preventing cyberstalking", *Journal of Business Ethics*, Vol. 145 No. 1, pp. 1-22.

Dhillon, G. and Torkzadeh, G. (2006), "Value-focused assessment of information system security in organizations", *Information Systems Journal*, Vol. 16 No. 3, pp. 293-314.

Dhillon, G., Oliveira, T., Susarapu, S. and Caldeira, M. (2016), "Deciding between information security and usability: developing value based objectives", *Computers in Human Behavior*, Vol. 61, pp. 656-666.

Drevin, L., Kruger, H.A. and Steyn, T. (2007), "Value focused assessment of information communication and technology security awareness in an academic environment", *Computers & Security*, Vol. 26 No. 1, pp. 36-43.

Eisenhardt, K.M. and Graebner, M.E. (2007), "Theory building from cases: opportunities and challenges", *The cademy of Management Journal*, Vol. 50 No. 1, pp. 25-32.

European Commission (2010), "Digitizing public services in Europe: putting ambition into action, 9th benchmark measurement", Directorate General for Information Society and Media, Unit C.4 Economic and Statistical Analysis, Bruxells.

Furnell, S., Sanders, P. and Warren, M. (1997), "Addressing information security training and awareness within the European healthcare community", *Studies in Health Technology and Informatics*, Vol. 43, pp. 707-711.

Gibson, J.L., Martin, D.K. and Singer, P.A. (2004), "Setting priorities in health care organizations: criteria, processes, and parameters of success", *BMC Health Services Research*, Vol. 4 No. 1.

Halperin, R. and Backhouse, J. (2008), "A roadmap for research on identity in the information society", *Identity in the Information Society*, Vol. 1 No. 1, pp. 71-87.

Hedström, K., Kolkowska, E., Karlsson, F. and Allen, J.P. (2011), "Value conflicts for information security management", *International Journal of Strategic Information Systems*, Vol. 20 No. 4, pp. 373-384.

Hedström, K., Karlsson, F. and Söderström, F. (2016), "Challenges of introducing a professional eID card within health care", *Transforming Government: People, Process and Policy*, Vol. 10 No. 1, pp. 26-46.

Hunter, M.G. (1997), "The use of RepGrids to gather data about information systems analysts", *Information Systems Journal*, Vol. 7 No. 1, pp. 67-81.

Holden, R.J., Carayon, P., Gurses, A.P., Hoonakker, P., Hundt, A.S., Ozok, A.A. and Rivera-Rodriguez, A.J. (2013), "SEIPS 2.0: a human factors framework for studying and improving the work of healthcare professionals and patients", *Ergonomics*, Vol. 56 No. 11, pp. 1669-1686.

Hutchinson, A., Young, T.A., Cooper, K.L., McIntosh, A., Karnon, J.D., Scobie, S. and Thomson, R.G. (2009), "Trends in healthcare incident reporting and relationship to safety and quality data in acute hospitals: results from the national reporting and learning system", *Quality and Safety in Health Care*, Vol. 18 No. 1, pp. 5-10.

Keeney, R.L. (1992), *Value-Focused Thinking*, Harvard University Press, Cambridge, MA.

Keeney, R.L. (1994), "Creativity in decision making with value-focused thinking", *Sloan Management Review*, Vol. 35 No. 4, pp. 33-41.

Keeney, R.L. (1999), "The value of internet commerce to the customer", *Management Science*, Vol. 45 No. 4, pp. 533-542.

Keeney, R.L. (2006), "Eliciting knowledge about values for public policy decisions", *International Journal of Information Technology & Decision Making*, Vol. 5 No. 4, pp. 739-749.

Keeney, R.L. (2013), "Foundations for group decision analysis", *Decision Analysis*, Vol. 10 No. 2, pp. 103-120.

Keeney, R.L. and Palley, A.B. (2013), "Decision strategies to reduce teenage and young adult deaths in the United States", *Risk Analysis : An Official Publication of the Society for Risk Analysis*, Vol. 33 No. 9, pp. 1661-1676.

Khan, M.K. and Kumari, S. (2014), "An improved user authentication protocol for healthcare services via wireless medical sensor networks", *International Journal of Distributed Sensor Networks*, Vol. 10 No. 4, pp. 347-169

Klein, H.K. and Myers, M.D. (1999), "A set of principles for conducting and evaluating interpretive field studies in information systems", *MIS Quarterly*, Vol. 23 No. 1, pp. 67-94.

Koved, L. and Zhang, B. (2014), "Improving usability of complex authentication schemes via queue management and load shedding", *Symposium on Usable Privacy and Security (SOUPS)*, *Citeseer*.

Lee, A.S. (1994), "Electronic mail as a medium for rich communication: an empirical investigation using hermeneutic interpretation", *MIS Quarterly*, Vol. 18 No. 2, pp. 143-157.

Li, M., Yu, S., Ren, K., Lou, W., (2010), "Securing personal health records in cloud computing: patient-centric and fine-grained data access control in multi-owner settings", in Jajodia, S. and Zhou, J. (Eds), *International conference on security and privacy in communication systems, Secure Commuity Springer*, *Berlin, Heidelberg*, pp. 89-106.

May, J., Dhillon, G. and Caldeira, M. (2013), "Defining value-based objectives for ERP systems planning", *Decision Support Systems*, Vol. 55 No. 1, pp. 98-109.

Merrick, J.R. and Garcia, M.W. (2004), "Using value-focused thinking to improve watersheds", *Journal of the American Planning Association*, Vol. 70 No. 3, pp. 313-327.

Merrick, J.R., Parnell, G.S., Barnett, J. and Garcia, M. (2005a), "A multiple-objective decision analysis of stakeholder values to identify watershed improvement needs", *Decision Analysis*, Vol. 2 No. 1, pp. 44-57.

Merrick, J.R., Grabowski, M., Ayyalasomayajula, P. and Harrald, J.R. (2005b), "Understanding organizational safety using value-focused thinking", *Risk Analysis*, Vol. 25 No. 4, pp. 1029-1041.

Mommens, P. (1999), "Ethical issues of health care in the information society", *Health Informatics Journal*, Vol. 5 No. 4, pp. 223-239.

Nelson, N.C. (2007), "Downtime procedures for a clinical information system: a critical issue", *Journal of Critical Care*, Vol. 22 No. 1, pp. 45-50.

Orlikowski, W.J. and Robey, D. (1991), "Information technology and structuring of organizations", *Information Systems Research*, Vol. 2 No. 2, pp. 143-169.

Phythian, G.J. and King, M. (1992), "Developing an expert system for tender enquiry evaluation: a case study", *European Journal of Operational Research*, Vol. 56 No. 1, pp. 15-29.

Pothier, D., Monteiro, P., Mooktiar, M. and Shaw, A. (2005), "Pilot study to show the loss of important data in nursing handover", *British Journal of Nursing (Mark Allen Publishing)*, Vol. 14 No. 20, pp. 1090-1093.

Power, D.J. and Sharda, R. (2007), "Model-driven decision support systems: concepts and research directions", *Decision Support Systems*, Vol. 43 No. 3, pp. 1044-1061.

Raghupathi, W. and Raghupathi, V. (2014), "Big data analytics in healthcare: promise and potential", *Health Information Science and Systems*, Vol. 2 No. 1.

Torkzadeh, G. and Dhillon, G. (2002), "Measuring factors that influence the success of internet commerce", *Information Systems Research*, Vol. 13 No. 2, pp. 187-204.

Walsham, G. (1995), "Interpretive case studies in IS research: nature and method", *European Journal of Information Systems*, Vol. 4 No. 2, pp. 74-81.

Walsham, G. and Waema, T. (1994), "Information systems strategy and implementation: a case study of a building society", *ACM Transactions on Information Systems*, Vol. 12 No. 2, pp. 150-173.

Witesman, E.M. and Walters, L.C. (2014), "Modeling public decision preferences using context-specific value hierarchies", *The American Review of Public Administration*, Vol. 45 No. 1, pp. 86-105.

Further reading

Angst, C.M., Devaraj, S., Queenan, C.C. and Greenwood, B. (2011), "Performance effects related to the sequence of integration of healthcare technologies", *Production and Operations Management*, Vol. 20 No. 3, pp. 319-333.

Sethi, N., Lane, G., Newton, S., Egan, P. and Ghosh, S. (2014), "Disaster easily averted? – data confidentiality and the hospital desktop computer", *International Journal of Medical Informatics*, Vol. 83 No. 5, pp. 385-391.

Corresponding author
Karin Hedström can be contacted at: karin.hedstrom@oru.se