

Information Security Goals in a Swedish Hospital

Ella Kolkowska, Karin Hedström, Fredrik Karlsson

MELAB, Swedish Business School at Örebro University, SE-701 82 Örebro, Sweden

ella.kolkowska@esi.oru.se, karin.hedstrom@oru.se, fredrik.karlsson@oru.se

Abstract. This paper presents findings of information systems security (ISS) goals found in policies, guidelines, and routines, i.e. in the formal system, at a Swedish hospital. The purpose of the paper is to analyze the ISS goals and relate them to confidentiality, integrity and availability (CIA) that are traditional objectives for managing ISS in organizations. A critical view on the CIA-triad has been taken in the study, to see how it is related to a hospital setting. Seven main ISS goals and 63 sub-goals supporting the main goals were identified. We found that the CIA-triad covers three of these main-goals. Confidentiality and integrity, however, have a broader definition in the hospital-settings than the traditional definitions. In addition we found four main ISS goals that the CIA-triad fails to cover. These are 'Follow ISS laws, rules and standards,' 'Traceability,' 'Standardized information' and 'Informed patients and/or family.' These findings contribute to the ongoing discussion about objectives in ISS management.

Keywords. Information Security, Health Care, Value, Goal

1 Introduction

Taking information systems security (ISS) issues in organizations seriously requires more than what traditional technology-centred security approaches can offer us (Dhillon & Backhouse, 2000; Siponen & Baskerville, 2001). Several scholars (e.g. Dhillon & Backhouse, 2001; Vroom & von Solms, 2004) have concluded that socio-technical aspects, such as goals and values held by individuals and organizations, are equally important. The consideration of such aspects seems to be especially important since a great number of security

incidents are caused by trusted personnel within organizations (Vroom & von Solms, 2004). Consequently, a more holistic view of information security problems and solutions is advocated in the area of information security (e.g., Dhillon & Backhouse, 2000; Dhillon & Backhouse, 2001; Siponen & Baskerville, 2001).

Dhillon and Backhouse (1996) argue that information security in organizations can be viewed as containing informal, formal and technical systems. The formal system consists of routines, policies, and guidelines for how information should be handled (Straub, 1990; R. Von Solms & Von Solms, 2004). The technical system is automated routines inside the formal system. Finally, the informal system consists of people's behaviours and communication. In a harmonic ISS solution the informal system supports the formal system; meaning that rules and procedures are accepted and adopted by the people in the organization (Dhillon, 2007).

Within the area of health care, Information and Communication Technology (ICT) is by many seen as way to increase patient security (e.g. Sveriges kommuner och landsting, Socialdepartementet, Läkemedelsverket, AB, & Carelink, 2006; Tsai & Bond, 2008). Although information security and protecting patient information has always been of high priority within the health care domain, the level of information security is still insufficient in this sector (Datainspektionen, 2005). An important aspect of health care work, which influences ISS, is the complex organization for delivering health care services. Health care involves many different collaborating and communicating actors, such as politicians, civil servants, care professionals, administrators, and managers. This complex structure leads to a varied and diverse work practice with many concurrent actors, actions, goals and values (Hedström, 2007; Åhlfeldt, 2006). People in every organization associate meaning to their action, and anchor them in goals and values (Rescher, 1969). As Dhillon (2007) states, goals and values in the informal system can be in conflict with goals and values found in the formal system. This concern becomes apparent when discussing organizations with strong professional cultures, such as a hospital (Scott, Mannion, Davies, & Marshall, 2003).

The research reported in this paper is part of a larger research project with the purpose to identify ISS value conflicts in health care, which will complement the study of Dhillon and Torkzadeh (2006), that focused general management values in respect to ISS. The purpose of this paper is to analyse ISS goals in the formal system of a Swedish hospital, and relate the ISS goals to the traditional objectives of ISS – the CIA-triad (confidentiality, integrity and availability). One problem with the CIA-triad is, as discussed further below, that the concepts are general objectives for the management of ISS, and as such not adapted to a specific organization. We therefore want to take a critical view on the CIA-triad and see how it is related to a hospital setting.

The paper is structured as follows. The following section describes the CIA-triad, its problems, and development of additional ISS objectives for the management of ISS in organizations. Section three gives an overview of the research method, followed by, in section four, a presentation of the ISS goals we found as a result of our analysis. The fifth section discusses our results, and the subsequent and last section, gives a short conclusion.

2 The CIA-triad

ISS is traditionally developed using the CIA-triad; confidentiality, integrity, and availability (Harris, 2002). These three objectives have guided the development of security measures to avoid different security threats in organizations. Confidentiality means that information assets are not accessible or revealed to unauthorized people. Integrity means that information assets are protected against undesired changes. The last concept, availability, means that information assets are accessible for the authorized users within the desired time (ISO/IEC 17799, 2005). Information assets include information itself and resources that are in use in managing the information (Oscarson, 2007).

However, the CIA triad has been criticized as insufficient in response to the new challenges that are emerging for information security (e.g. Anderson, 2002; Dhillon & Backhouse, 2000; Dhillon & Torkzadeh, 2006; Harris, 2002). The most central critique of the CIA-triad is its ignorance of the complicated socio-organizational context of managing information security in an organization (e.g. Anderson, 2002; Dhillon & Backhouse, 2000; Tormpeter & Eloff, 2001). It has for instance been argued that objectives may be related to a specific type of organization as different types of organizations vary in terms of goals, strategies, structures and cultures (R. Von Solms & Von Solms, 2004). Consequently, researchers in the information security area argue that the traditional objectives should be complemented by additional objectives that make it possible to deal with ethical, social, and organizational aspects of information handling in organizations (e.g. Dhillon & Backhouse, 2000; Dhillon & Torkzadeh, 2006; Tormpeter & Eloff, 2001)

One attempt to find additional objectives for information security is a study of Dhillon and Backhouse (2000). They suggest that the traditional concepts should be complemented by four new principles; responsibility, integrity, trust and ethicality (RITE). These principles are not really objectives, but can be viewed as areas to consider when managing ISS in organizations. Responsibility means having knowledge of rules and understanding of responsibilities. Based on that knowledge, members of an organization are able to develop their own security practices when needed and that these practices are in line with overall organizational rules. Integrity means being moral sound and loyal to the organization. In an ISS context trust means that relationships within organizations

should be built on confidence rather than control. For example, employees have to be trusted to act according to the organization's norms and accepted behavior patterns. Furthermore, employees have to feel confident that their privacy will not be compromised by too strict security controls. Ethicality means that members of an organization should act according to ethical principles instead of strictly follow formal rules. The latter principle is supported by Trompeter and Eloff (2001), they emphasize the importance of consideration of ethical principles when deciding on principles for ISS.

In addition, responsibility has later received a wider interpretation (Dhillon, 2007; Moulton & Coles, 2003). They point at the importance of taking both internal and external organizational contexts into consideration when discussing responsibility. This means, for example, that organizations are accountable to its partners and clients and to follow laws and regulations issued by the government.

Another attempt to improve the ISS management is a study by Dhillon and Torkzadeh (2006). They studied security managers' values related to ISS and transformed them to objectives that are essential in protecting organizations' information resources. Their study shows that the CIA-triad is only a small part of all possibly objectives in the management of ISS. Objectives such as maximizing awareness, developing and sustaining an ethical environment, enhance integrity of business processes, maximizing of data integrity, maximizing organizational integrity, and maximizing privacy are also important in managing ISS within organizations. Many of the identified objectives are not only important to ensure information security but are part of the corporate governance. This is in line with other researchers who point out the importance of considering information security issues in relation to corporate governance and not as isolated processes in the organization (e.g., Dhillon, 2007; McFadzean, Ezingear, & Birchall, 2006; B. von Solms, 2006; Basie. von Solms & von Solms, 2005).

3 Research method

This study was carried out at the hospital of Karlskoga – a small Swedish county hospital in central Sweden. The hospital serves approximately 90 000 citizens. The hospital is situated in the County of Örebro, responsible for healthcare for 274 000 inhabitants. There are, apart from Karlskoga hospital, two more hospitals and several primary care clinics in the County of Örebro.

The purpose of this paper is, as we wrote in the Introduction, to analyse ISS goals in the formal system of a Swedish hospital and compare these goals with the CIA-triad. The analyzed ISS goals are found in official documents related to ISS. As we mentioned before, this study is a part of a larger research project with the aim to identify value conflict between formal and informal values in health care. The document analysis presented in this paper is the first phase of this project and

the study will later be complemented with interviews and observations at the hospital.

We decided to focus our study on ISS goals related to patient information, as treating patients is hospitals' main activity. In addition, we used the County of Örebro's overall goal for ISS as our working definition of ISS, and subsequently as demarcation in the analysis: 'Correct information to the right people, right on time, and to the right place.'

The operationalization of the case study method is based on a research method used by Dhillon and Torzadeh (2006) with the purpose of identifying ISS objectives. The qualitative research method can be divided into three steps, which have been carried out iteratively:

- (1) Identifying formal ISS goals – the process began with document analysis, to identify goals in the formal system, as represented by organisational ISS goals and routines on the county council level as well as hospital level. Goal statements were numbered and listed in a database. The following documents were analysed:
 - a. County council information security policy
 - b. County council IT strategy
 - c. Information to county council staff about information security
 - d. Security instructions for county council IT users
 - e. IT policy for the county council
 - f. County council policy for information and communication
 - g. Routines for handling medical records at Karlskoga hospital.
- (2) Structuring goals – first, we structured all statements in order to eliminate duplicates. Second, we sorted the goals into identified clusters. For each cluster we elicited a main goal, which was used as constituted the cluster's demarcation. We reformulated the goals expressed in the documents to make them more concise. The main goal g61 'Follow ISS laws, rules and standards', and goal g87 'Informed patients and/or family' were not found in the reviewed documents, but rather generalizations of its underlying sub-goals.
- (3) Organizing objectives – in order to structure the goals we identified the relationships between the main goals and the sub-goals. We illustrated this using goal graphs inspired by Yu (1993). The goal-graphs were jointly developed by the researchers in order to minimize biases. To ensure traceability each goal is related, by one or several and letters to the specific document(s) where the goal is found. The letter(s) refers to the documents in the list above, and 'a', for example, relates to the County council information security policy.

4 Formal ISS goals in a Swedish hospital

In this analysis we present the formal ISS goals we found in the hospital's policy and routine documents. The goals are analyzed in the form of goal-graphs (Yu, 1993) where main goals are related to sub-goals. The sub-goals are means to achieve the main goals.

The main ISS goals are 'Complete confidentiality,' 'Available information,' 'Traceability,' 'Reliable information,' 'Standardized information,' 'Follow ISS laws, rules, and standards' and 'Informed patients and/or family.'

4.1 Complete confidentiality

Figure 1 illustrates the main goal Goal 1 'Complete confidentiality.' The purpose of 'Complete confidentiality' is to ensure that only authorized people can access sensitive information about a patient, and that only necessary healthcare information about the patient is shared and discussed.

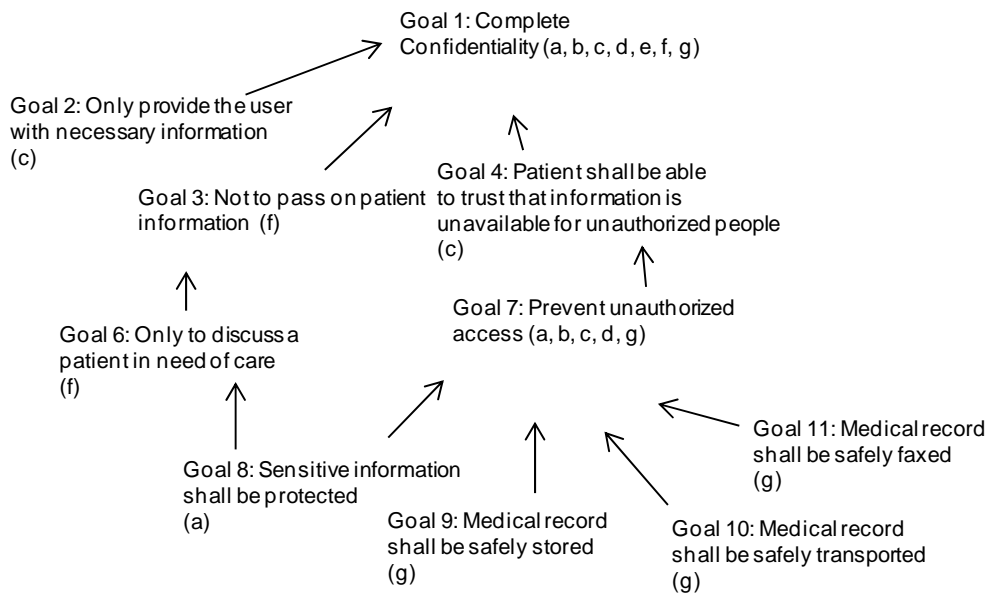


Figure 1: Goal graph – complete confidentiality

The goal 'complete confidentiality' (Goal 1) is important in hospital settings and has been found in all analyzed documents. Confidentiality is in our setting related to information handled by the computer system, manual information handling as well as to spoken communication between staff. One part of the goal is related to protecting patients' information from disclosure to unauthorized people (Goal 4, Goal 7, Goal 11, Goal 10, Goal 9). The other part of the goal is related to handling of patient's information by authorized users (Goal 2, Goal 3,

Goal 6, Goal 8). The central purpose for ‘complete confidentiality’ is respect to the patients and their privacy, as can be seen in goal g4 ‘Patient shall be able to trust that sensitive information is unavailable for unauthorized people.’ This sub-goal is achieved by realizing goal Goal 7, ‘Prevent unauthorized access’, which is emphasized in the analyzed documents. This goal is related to both information in computerized information systems (Goal 8) and information in paper-based records (Goal 11, Goal 10, Goal 9). Suggested security measures are, for example, routines how to handle paper-based patients’ records when they are used, stored, transported and faxed. Two other goals that support the main goal ‘complete confidentiality’ are Goal 2 and Goal 3. These goals are related to how authorized people should handle sensitive information about patients. The only information that should be communicated is information related to the health care.

4.2 Available information

In Figure 2 we have illustrated the main goal (Goal 13), ‘Available information.’ Available information means that healthcare professionals should have access to information when needed. This is crucial in a healthcare situation. Without access to relevant, as well as correct, information, there is a risk for the patient’s health.

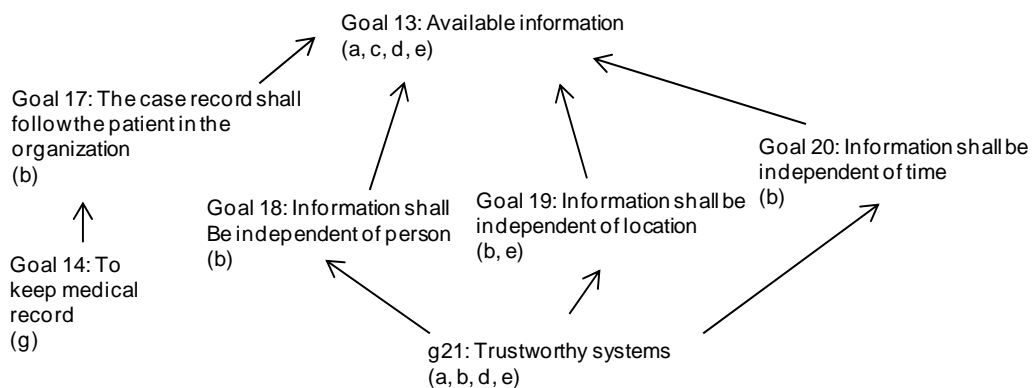


Figure 2: Goal graph – available information

According to the analyzed documents the goal ‘available information’ can be achieved when information is independent of person (Goal 18), time (Goal 20) and location (Goal 19) and when medical records follow the patient in the organization (Goal 17). However, in order to achieve these goals the documents state two prerequisites: the hospital has to keep medical records (Goal 14) and that the systems have to be trustworthy (Goal 21). In order to achieve these goals information technology is viewed as a means, where electronic health records can be made available independent of place, person and time.

4.3 Traceability

In Figure 3, we illustrate the main goal (Goal 30), ‘Traceability.’ This goal means that actions and decisions concerning the flow of information, in the information system, shall be traceable through logging and documentation.

The traceability goal is related to both manual handling of information and computerized information systems. Traceability related to computer systems emphasizes tracing performed actions in the systems to the responsible actors (Goal 32). This is important in hospital settings because most of the users can access more information than they actually need for their work. The solution is a balance between security and flexible access to information. Thus to prohibit misuse of these rights in the system, traceability of user actions is extremely important. Traceability is in this case ensured by logging, supervision of the networks (Goal 33) and use of digital signatures (Goal 89). Another part of traceability in the hospital setting is related to tracing information. This mostly concerns paper-based medical records, in order to know where the records are. Goals 37 to 43 concern the use of copies, the request of medical records and whether information have reached the desired destination and/or people.

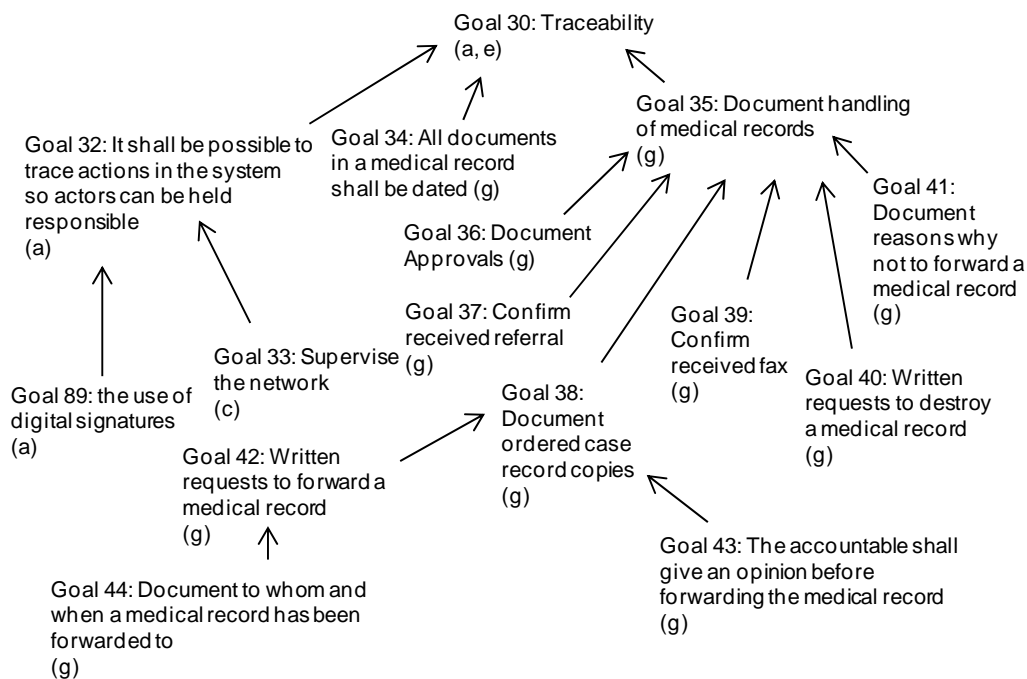


Figure 3: Goal graph – traceability

4.4 Reliable information

The main goal ‘Reliable information’ (Goal 15) is illustrated in Figure 4. Reliable information means that information should be correct; i.e., intact as well as

updated. To have access to reliable information is very important in a hospital environment. Incorrect information could hurt patients, or even be fatal.

Intact information means that the information should not be distorted (Goal 23) by desired or undesired changes (Goal 24, Goal 28), and that information should be protected against losses (Goal 29). Improving users' IT skills and knowledge about information security (Goal 90 and Goal 25) shall prevent accidental losses and also by improving transmission of information between different receivers (Goal 28). In addition, reliable and correct information also means that the information is updated. In the case of paper-based medical record it means that documents about the patient are added to the record (Goal 26) and the documents in the record are sorted continuously (Goal 27). Hence outdated documents are removed from the record and the documents are placed a specific order.

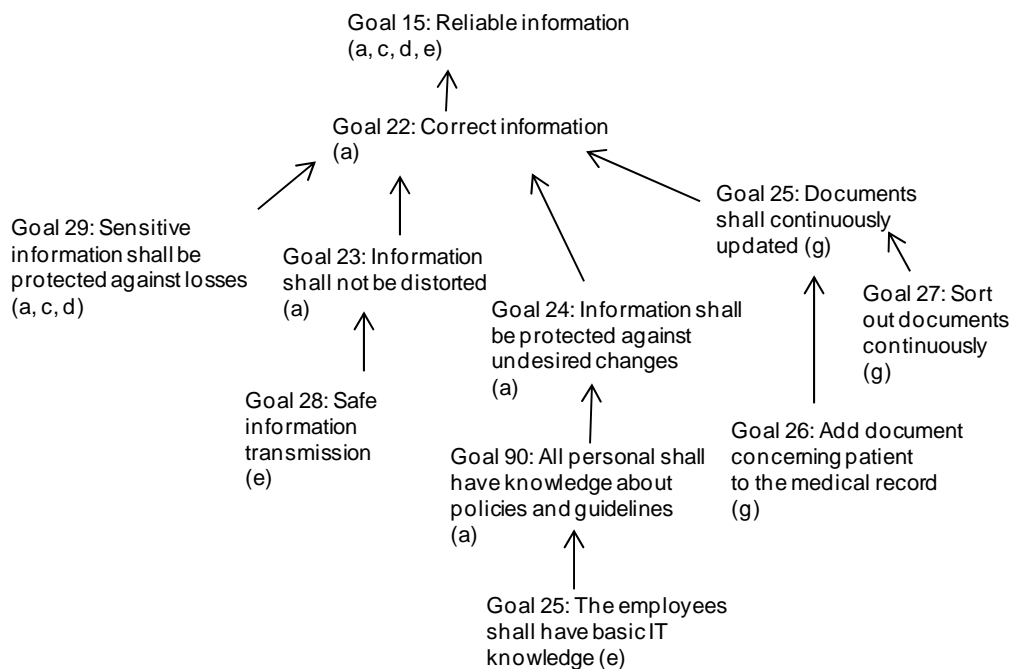


Figure 4: Goal graph – reliable information

4.5 Standardized information

The goal graph in Figure 5 describes the underlying structure of Goal 45: 'Standardized information'. Goal 45 illustrates the importance of using the same structure and concepts when recording information. This is important in order to facilitate a unified interpretation of the information.

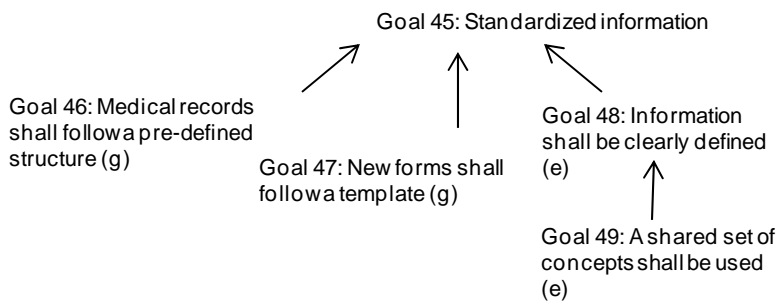


Figure 5: Goal graph – standardized information

According to our analysis the goal ‘Standardized information’ is achieved when medical records follow a pre-defined structure (Goal 46), when forms follow given and standardized templates (Goal 47) and finally when information is clearly defined (Goal 48). The last goal is elaborated even further stating that information is clearly defined when used concepts are shared by the personnel (Goal 49).

4.6 Follow ISS laws, rules, and standards

Figure 6 illustrates the main goal ‘Follow ISS laws, rules, and standards’ (Goal 61). This goal points at the importance of healthcare organizations following prescribed security ISS regulations, laws regulating healthcare and information use, as well as ISS standards and classifications, as support for managing ISS.

There are a number of important laws and regulations that have to be followed in the work at the hospital and not least in the work with information security (Goal 64). We find that goals number 5, 62 and 63 is related to law issues on how to handle privacy of patients and access to official documents. These goals influence the work with information security because they are related to how patient information should be handled. Other sub-goals emphasized in the analyzed document are stressing structured work with information security (Goal 69) by the use of international standards (Goal 65). These standards should guide classification of information (Goal 67, Goal 71) and the implementation of security measures (Goal 70, Goal 72). Another important sub-goal in this context is that the rules and policies have to be known and followed (Goal 68). According to the analyzed document this will be achieved by distributing relevant acts (Goal 66), education about information security (Goal 73) and creating a risk awareness in the organization (Goal 74).

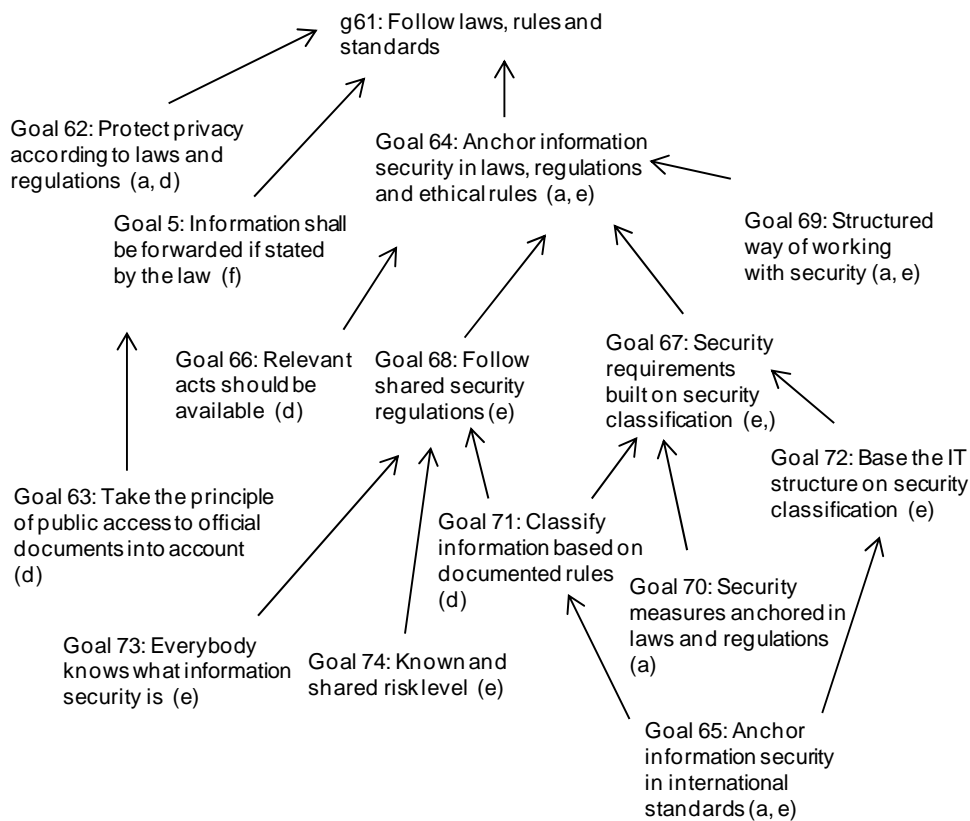


Figure 6: Goal graph – Follow ISS laws, rules, and standards

4.7 Informed patients and/or family

The main, and final, goal illustrated in Figure 7 is Goal 87: ‘Informed patients and/or family’. This goal points at the importance of making sure that patients and his/her family have information about his/her health status (Goal 86, Goal 84). This includes where treatment is going to take place, information regarding different treatments, as well as information about forwarding of the medical record (Goal 82).

Furthermore ‘Informed patients and/or family’ means that the patient has a right to decide about disclosure of his/her medical records (Goal 78). The patient has to approve before passing of the medical record (Goal 79, Goal 80) to other receivers or before making copies of the medical records.

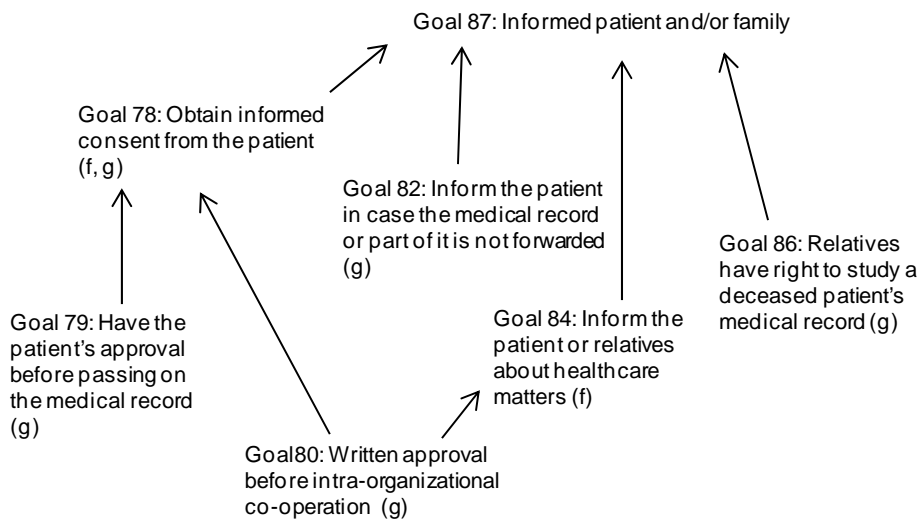


Figure 7: Goal graph – informed patients and/or family

5 Discussion

The purpose of this paper was to critically examine the objectives that traditionally are used to manage ISS in organizations; confidentiality, integrity, and availability, and relate them to the formal ISS-goals found in the study. If we recapture these concepts confidentiality means that information assets has to be protected and not accessible or revealed to unauthorized people. The objective of integrity is to protect information assets against unwanted changes. The purpose of the last concept, availability, is to assure that information assets are accessible for the authorized users within the desired time.

If we take a closer look at the goal-graphs illustrated in Figures 1 to 7 above, we find that the CIA-triad covers three of the main-goals found in the documents from Karlskoga hospital. ‘Complete confidentiality’ found in Figure 1, has a similar interpretation as confidentiality, found in the CIA-triad. The focus is on that sensitive medical information shall only be disclosed to authorized people. However, the sub-goals related to ‘Complete confidentiality’ emphasize also the importance of handling patient’s information with respect to patient’s privacy and only share and discuss information related to health care matters (Goal 3 and Goal 6). This part of the concept is related to how authorized users should handle patient’s information and is related to the earlier discussed principle of responsibility suggested by Dhillon and Backhouse (2000) as a complement to CIA.

The second CIA-concept, integrity, is similar to the meaning of the main goal ‘Reliable information’ illustrated in detail in Figure 4. ‘Reliable information’ has in the hospital-setting, however, a wider definition than only to protect information against undesired changes. Here it also points at the importance of

keeping information updated (Goal 25), understandable (Goal 23) and sorted (Goal 27).

Finally, the third CIA-concept, availability, has the same meaning as the main goal 'Available information' in Figure 2. Both objectives aim to make sure that information is accessible irrespective of time or place.

But, the CIA-triad fails to cover the other ISS-goals we found in the formal documents from Karlskoga hospital. These are 'Follow ISS laws, rules and standards,' 'Traceability,' 'Standardized information' and 'Informed patients and/or family.'

'Traceability' means that actions and decisions concerning the flow of information, in the information system, shall be possible to trace through logging and documentation. The need of tracing and deriving an actor's performed actions is emphasized in the ISS field. Accountability (identification, authentication or authorization) has been suggested as a complement to CIA (Harris, 2002; Oscarson, 2007). However 'Traceability' found in the hospital document has much broader meaning than accountability. 'Traceability' emphasizes the importance of tracing information (e.g. Goal 34), and not only trace the individuals that produce the information.

Remaining main ISS goals found in the study 'Follow ISS laws, rules, and standards,' 'Standardized information' and 'Informed patients and/or family' can be related the broader interpretation of responsibility (Dhillon, 2007). The goals we have identified show that the hospital has responsibilities to other actors.

During the analysis of the documents related to information handling and ISS at the hospital we have also identified a number of business goals that make a context for ISS goals at the hospital. These business goals are: 'Efficient healthcare,' 'Correct healthcare,' 'Empowered patients' and 'Individualized healthcare.' We can see that the ISS goals contribute to the business goals. For example, 'Efficient healthcare' is supported by the ISS-goal 'Standardized information' analysed in Figure 5. The business goal 'Correct healthcare' is supported by the ISS-goals 'Available information' (Figure 2), and 'Reliable information' (Figure 4). Another business goal, supported by ISS-goals, is 'Empowered patients.' This goal is supported by the goal 'Informed patients and/or family' illustrated in Figure 7. We consider it important that the ISS goals are associated to the business context in order to maintain the integrity of the organization. This is in line with earlier research that points out the importance of considering information security issues in relation to corporate governance (e.g., Baskerville & Siponen, 2002). However the relationship between business goals and ISS goals was not fully elaborated in our study and need further analysis.

6 Conclusion

The purpose of this paper was to analyse information systems security (ISS) goals in the formal system of a Swedish hospital, and relate the ISS-goals to the traditional objectives of ISS – the CIA-triad (confidentiality, integrity and availability). A critical view on the CIA-triad was taken in this study to see how it is related to a hospital setting. The main problem with the CIA-triad is that these goals are general, and as such not adapted to a specific organization or type of organization. Hence, the CIA-triad fails to cover organizational specific ISS aspects of a hospital.

Seven main ISS goals were identified in this study. These goals are ‘Complete confidentiality,’ ‘Available information,’ ‘Traceability,’ ‘Reliable information,’ ‘Standardized information,’ ‘Follow ISS laws, rules, and standards’ and ‘Informed patients and/or family.’ Three of the goals – ‘Complete confidentiality,’ ‘Available information,’ ‘Reliable information’ – correspond to the CIA-triad, although they have a somewhat broader definitions than the traditional definitions. Consequently, these goals show that the original objectives need to be adapted to the hospital settings.

The additional four objectives – ‘Traceability,’ ‘Standardized information,’ ‘Follow ISS laws, rules, and standards’ and ‘Informed patients and/or family’ – are not found in the CIA-triad. However, they can be related to complementing principles that have been identified in the ISS field. Consequently, our findings from the hospital setting contribute to the ongoing discussion about objectives in the holistic view of ISS.

References

- Anderson, J. (2002). "Why we need a new definition of Information Security", *Computer & Security*, vol. 22, no. 4, 308-313.
- Baskerville, R., & Siponen, M. (2002). "An information security meta-policy for emergent organizations", *Logistics Information Management*, vol. 15, no. 5/6, 337-346.
- Datainspektionen. (2005). *Ökad tillgänglighet till patientuppgifter* (No. 2005:1).
- Dhillon, G. (2007). *Principles of information systems security: text and cases*. Wiley Inc., Hoboken, NJ.
- Dhillon, G., & Backhouse, J. (1996). "Risks in the Use of Information Technology Within Organizations", *International Journal of Information Management*, vol. 16, no. 1, 65-74.
- Dhillon, G., & Backhouse, J. (2000). "Information security management in the new millenium", *Communication of the ACM*, vol. 43, no. 7, 125-128.
- Dhillon, G., & Backhouse, J. (2001). "Current directions in IS security research: towards socio-organisational perspectives" *Information Systems Journal*, vol. 11, no. 2.
- Dhillon, G., & Torkzadeh, G., (2006). "Value-focused assessment of information security in organizations", *Information Systems Journal*, vol. 16, no. 3, 293-314.
- Harris, S. (2002). *CISSP All-in-one Certification Exam Guide*. McGraw-Hill/Osborne, New York.
- Hedström, K. (2007). "The Values of IT in Elderly Care", *Information Technology & People*, vol. 20, no. 1, 72-84.

- ISO/IEC 17799. (2005). ISO/IEC 27002:2005 Information Technology - Security Techniques - Code of Practice for Information Security Management. International Organization for Standardisation (ISO), www.iso.org.
- McFadzean, E., Ezingard, J.-N., & Birchall, D. (2006). "Anchoring Information Security Governance Research: Sociological Groundings and Future Directions", *Journal of Information System Security*, vol. 2, no. 3.
- Moulton, R., & Coles, R. S. (2003). "Applying information security governance", *Computers and Security*, vol. 22, no. 7, 580-584.
- Oscarson, P. (2007). *Actual and perceived information systems security*. Linköping University, Linköping, Sweden.
- Rescher, N. (1969). *Introduction to value theory*. Prentice-Hall, Englewood Cliffs.
- Scott, T., Mannion, R., Davies, H., & Marshall, M. (2003). "Implementing culture change in health care: theory and practice", *International Journal for Quality in Health Care*, vol. 15, 111-118.
- Siponen, M., & Baskerville, R. (2001). A new paradigm for adding security into IS development methods. In J. Eloff, L. Labuschagne, R. Solms & G. Dhillon (Eds.), *Advances in information security management & small systems security*, pp. 99-111, Kluwer Academic Publishers, Boston.
- Straub, D. (1990). "Effective IS security: an empirical study", *Information System Research*. 1(2). Sveriges kommuner och landsting, Socialdepartementet, Läkemedelsverket, AB, A., & Carelink.
- (2006). Nationell IT-strategi för vård och omsorg: Socialdepartementet.
- Tormpeter, C. M., & Eloff, J. (2001). "A framework for implementation of socio-ethical controls in information security", *Computers & Security*, vol. 20, no. 5, 384-391.
- Tsai, J., & Bond, G. (2008). "A comparison of electronic records to paper records in mental health centers", *International Journal for Quality in Health Care*, vol. 20, no. 2, 136-143.
- von Solms, B. (2006). "Information Security - The Fourth Wave", *Computers & Security*, 25, no. 3, 165-168.
- von Solms, B., & von Solms, R. (2005). "From information security to....business security?", *Computers & Security*, 24, 271-273.
- Von Solms, R., & Von Solms, B. (2004). "From policies to culture", *Computers and Security*, 23(4), 275-279.
- Vroom, C., & von Solms, R. (2004). "Towards information security behavioural compliance", *Computers and Security*, 23(3), 191-198.
- Yu, E. (1993). *Modelling Organizations for Information Systems Requirements Engineering*. Paper presented at the The IEEE International Symposium on Requirements Engineering, San Diego, California, USA.
- Åhlfeldt, R.-M. (2006). *Information Security in a Distributed Healthcare Domain Exploring the Problems and Needs of Different Healthcare Providers* Stockholm University, Stockholm.