Annual Security Conference
Discourses in Security Assurance & Privacy

Security, Assurance and Privacy: Organizational Challenges
Proceedings of the 8th Annual Security Conference
Discourses in Security Assurance & Privacy
Las Vegas, NV, USA
April 15-16, 2009

Editor
Gurpreet Dhillon
Virginia Commonwealth University, USA

ISBN: 978-1-935160-04-5

www.security-conference.org

Information Security Goals in a Swedish Hospital

Ella Kolkowska, Karin Hedström, Fredrik Karlsson
Örebro University, Sweden

Abstract

One of the problems highlighted within the area of information security is that internatonal standards are implemented in organisations without adopting them to special organisational settings. This paper presents findings of information security goals found in policies, guidelines, and routines at a Swedish hospital. The purpose of the paper is to analyze the information security goals and relate them to confidentiality, integrity and availability (CIA) that are traditional objectives for managing information security in organisations. 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 information security 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-setting than the traditional definitions. In addition, we found four main information security goals that the CIA-triad fails to cover. These are 'Follow information security laws, rules and standards,' 'Traceability,' 'Standardized information' and 'Informed patients and/or family.' These findings shows that there is a need to adopt the traditional information security objective to special organisational settings.

Keywords: *Information Security, Health Care, Value, Goal*

Introduction

Taking information security issues in organisations seriously requires more than what traditional technology-centred security approaches can offer us (Dhillon & Backhouse, 2000; Siponen & Baskerville, 2001). Although approaches that considers social and organisational aspects in information security has become more common in the field during the last fifteen years there is still a need for more studies of social aspects in relation to information security (Thomson, von Solms, & Louw, 2006; Von Solms & Von Solms, 2004; Vroom & von Solms, 2004) and also there is a need for more studies of organisational aspects concerning how to integrate information security with other organisational processes (Anderson, 2002; von Solms, 2006; von Solms & von Solms, 2005).

One of the trends in the information security field under the last decennium has been standardization, certifications and development of best practices for information security in organisations (Von Solms, 2000). This trend was an answer for security management's needs for knowing what a sufficient level of information security in organisation is, and verifying the sufficient level of information security for the organisation's partners. The most known and widespread standard today is the international standard ISO/IEC 17799 – Information Security Code of Practice (ISO/IEC 17799, 2005) (Freeman, 2007).
However just applying international codes of practices in organisation cannot ensure which controls are needed in every specific situation, because the standards are rather a kind of baseline for information security (Von Solms & Von Solms, 2004). In a specific situation the special context to the IT environment should be taken into account when the standard are applied, in order to establish unique information security requirements

of an organisation (Gerber & von Solms, 2005). The problem is that many organisations just apply the standard without addressing the special security needs of the specific organisation (Thomson & von Solms, 2006).

Information security is an important issue within the area of health care. In this area 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 information security, is the complex organisation for delivering health care services. Health care involves many different collaborating and communicating actors, such as politicians, civil servants, health care professionals, administrators, and managers on different levels. This complex structure leads to a varied and diverse work practice with many concurrent actors, actions, goals and values (Hedström, 2007; Åhlfeldt, 2006). The different actors inscribed different values in policies, guidelines and other strategic documents that influence work with information security.

The purpose of this paper is to analyse information security goals identified at a Swedish hospital, and relate the information security goals to the traditional objectives of information security – the CIA-triad (confidentiality, integrity and availability) pointed out in the international standard. One problem with the CIA-triad is, as discussed further below, that the concepts are general objectives for the management of information security, and as such not adapted to a specific organisation. 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 objectives for the management of information security in organisations. Section three gives an overview of the research method, followed by, in section four, a presentation of the information security 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

The CIA-triad

Concepts used to relate security in context of IT and IS in international standards is information security. According to (ISO/IEC 17799, 2005), *information security means "preservation of confidentiality, integrity and availability of information*" (ISO/IEC 17799, 2005). These three objectives have guided the development of security measures to avoid different security threats in organisations. Confidentiality means that information is not accessible for unauthorized people. Integrity means that information is protected against undesired changes. The last concept, availability, means that information is accessible for the authorized users within the desired time (ISO/IEC 17799, 2005). However, both the concept of information security and 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; e.g. Harris, 2002). Their critique concern the definition and the objectives. The CIA triad fail to relate information security to an organizational and business context, and there insufficient emphasis on the organisational actors' roles in working with information security (e.g. Anderson, 2002; Dhillon & Torkzadeh, 2006; e.g. von Solms & von Solms, 2005). Two concepts that are suggested to replace the information security concept are business security (von Solms & von Solms, 2005), and Information system security (IS security) (Dhillon, 1997). Business security emphasizes the relation of security work with other organisational processes (von Solms & von Solms, 2005), and IS security emphasizes the holistic and contextual view of security by not only focusing information, but views the whole information system as a protection object (Dhillon, 2007). Consequently, due to the wider definition, 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 organisational aspects of information handling in organisations and better support the new challenges of business security and IS security. (e.g. Dhillon & Backhouse, 2000; Dhillon & Torkzadeh, 2006; Tormpeter & Eloff, 2001)

One attempt to find additional objectives for IS 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 information security in organisations. Responsibility means having knowledge of rules and understanding of responsibilities. Based on that knowledge, members of an organisation are able to develop their own security practices when needed and that these practices are in line with overall organisational rules. Integrity means being moral sound and loyal to the organisation. In an IS security context trust means that relationships within organisations should be built on confidence rather than control. For example, employees have to be trusted to act according to the organisation'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 organisation 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 IS security. In addition, responsibility has later received a wider interpretation. A number of scholars have pointed at the importance of taking both internal and external organisational contexts into consideration when discussing responsibility (Dhillon, 2007; Moulton & Coles, 2003). This means, for example, that organisations are accountable to its partners and clients and to follow laws and regulations issued by the government.

Another attempt to improve the information security management is a study by Dhillon and Torkzadeh (2006). They studied security managers' values related to IS security and transformed them to objectives that are essential in protecting organisations' information resources. Their study shows that the CIA-triad is only a small part of all possibly objectives in the management of IS security. Objectives such as maximizing awareness, developing and sustaining an ethical environment, enhance integrity of business processes, maximizing data integrity, maximizing organisational integrity, and maximizing privacy are also important in managing IS security within organisations. Many of the identified objectives are not only important to ensure IS 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 organisation (e.g., Dhillon, 2007; McFadzean, Ezingeard, & Birchall, 2006; von Solms, 2006; e.g., von Solms & von Solms, 2005).

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 identify information security goals at a Swedish hospital and compare these goals with the CIA-triad. The analyzed information security goals are found in official documents related to information security and information handling. We decided to focus our study on information security goals related to patient information, as treating patients is hospitals' main activity. In addition, we used the County of Örebro's overall goal for information security as our working definition of information security, and subsequently as demarcation in the analysis: 'Correct information to the right people, right on time, and to the right place.' The case study method is based on a research method used by Dhillon and Torkzadeh (2006) with the purpose of identifying IS security objectives. The qualitative research method can be divided into three steps (identifying information security goals, structuring goals, and organising objectives), which have been carried out iteratively:

1. Identifying information security goals – the process began with document analysis, to identify goals, as represented by organisational information security goals and routines on the county council level as well as hospital level. The different documents were chosen in order to capture different actors' goals related to information security and not just information security managers goals espoused in information security policy. This was important because of the complex organisation for delivering health care services, which involves many different collaborating and communicating actors. Goal statements were numbered and listed in a database. Seven main information security goals and 63 sub-goals supporting the main goals were identified in the study. 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 below. Second, we sorted the goals into identified clusters. For each cluster we elicited

a main goal, which constituted the cluster's demarcation. For example goals such as "provide user with only necessary information", "only discuss patient in need of care", "prevent unauthorized access" deal with similar issue, i.e., confidentiality, which made us sort them the cluster "complete confidentiality". We reformulated the goals expressed in the documents to make them more concise.

3. Organizing objectives – in order to structure the goals we identified the relationships between the main goals and the sub-goals within each cluster. We illustrated this using goal graphs inspired by Yu (1993). During the analysis seven goal graphs were identified: "complete confidentiality", "Available information", Traceability", "Reliable information", "Standardized information", "Follow information security laws, rules, and regulations", Informed patients and/or family". Each goal-graph was 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

Information security goals in a Swedish hospital

In this analysis we present the information security 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 information security goals are 'Complete confidentiality,' 'Available information,' 'Traceability,' 'Reliable information,' 'Standardized information,' 'Follow information security laws, rules, and standards' and 'Informed patients and/or family.'

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.

The goal 'complete confidentiality' 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. The other part of the goal is related to handling of patient's information by authorized users. The central purpose for 'complete confidentiality' is respect to the patients and their privacy, as can be seen in goal 'Patient shall be able to trust that sensitive information is unavailable for unauthorized people.' This sub-goal is achieved by realizing goal, 'Prevent unauthorized access', which is emphasized in the analyzed documents. This goal is related to information in computerized information systems and information in paper-based records. 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 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

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. The goal is emphasized in all analyzed documents. According to the analyzed documents the goal 'available information' can be achieved when information is independent of person, time, and location, and when medical records follow the patient in the organisation. However, in order to achieve these goals the documents state two prerequisites: the hospital has to keep medical records and that the systems have to be trustworthy. 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.

Traceability

'Traceability' means that actions and decisions concerning the flow of information, in the information system, shall be traceable through logging and documentation. This goal is mainly emphasized in two documents: County council information security policy (a) and routines for handling medical records at Karlskoga hospital (g). 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. 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 and use of digital signatures. 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. Six sub-goals concern the use of copies, the request of medical records and whether information has reached the desired destination and/or people.

Reliable information

The main goal '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. This goal is emphasized in County council information security policy, Security instructions for county council IT users, Security instructions for county council IT users, Routines for handling medical records at Karlskoga hospital. Intact information means that the information should not be distorted by desired or undesired changes, and that information should be protected against losses. Improving users' IT skills and knowledge about information security shall prevent accidental losses and also by improving transmission of information between different receivers. 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 and the documents in the record are sorted continuously. Hence outdated documents are removed from the record and the documents are placed a specific order.

Standardized information

'Standardized information', 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. This goal is emphasized in IT policy for the county council and in Routines for handling medical records at Karlskoga hospital. According to our analysis the goal 'Standardized information' is achieved when medical records follow a pre-defined structure, when forms follow given and standardized templates and finally when information is clearly defined. The last goal is elaborated even further stating that information is clearly defined when used concepts are shared by the personnel.

Follow information security laws, rules and standards
'Follow information security laws, rules, and standards' is emphasized mainly in County council information security policy and IT policy for the county council, but it is mentioned even in other documents like: Security instructions for county council IT users and County council policy for information and communication. This goal points at the importance of healthcare organisations following prescribed security information security regulations, laws regulating healthcare and information use, as well as information security standards and classifications, as support for managing information security.

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. We find that three goals are 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 by the use of international standards. These standards should guide classification of information and the implementation of security measures. Another important sub-goal in this context is that the rules and policies have to be known and followed. According to the analyzed document this will be achieved by distributing relevant acts, education about information security and creating organizational risk awareness.

Informed patient and/or family

The main, and final, goal: 'Informed patients and/or family' points at the importance of making sure that patients and his/her family have information about his/her health status. This includes where treatment is going to take place, information regarding different treatments, as well as information about forwarding of the medical record. Furthermore 'Informed patients and/or family' means that the patient has a right to decide about disclosure of his/her medical records. The patient has to approve before passing of the medical record to other receivers or before making copies of the medical records. This goal is emphasized in County council policy for information and communication and Routines for handling medical records at Karlskoga hospital

Discussion

The purpose of this paper was to critically examine the objectives that traditionally are used to manage information security in organisations; confidentiality, integrity, and availability (described in section 2), and relate them to the information security goals found in the study. Different strategic documents related to information handling and information security have been analyzed in the study to capture different actors' goals related to information security. It has been described earlier that one characteristic feature of hospital settings is a complex organisation with many different collaborating and communicating actors such as politicians, civil servants, healthcare professionals, administrators, patients, and managers. Many of the actors are responsible for creating policies and guidelines related to information security and information handling.

If we take a closer look at main goals described in section 4 above, we find that the CIA-triad covers three of the main-goals found in the documents from Karlskoga hospital. 'Complete confidentiality' has a similar interpretation as confidentiality, found in the CIA-triad. This means 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. This is not really covered by 'confidentiality' in information security standards, but can be related to the earlier discussed principle of responsibility suggested by Dhillon and Backhouse (2000) as a complement to CIA. This part of the of the concept is also related to the wider discussed aspect of responsibility (Moulton & Coles, 2003) that emphasizes organisational accountability to its partners and clients, here patients in hospital settings. The second CIA-concept, integrity, is similar to the meaning of the main goal 'Reliable information'. '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, understandable, and sorted. This goal is strongly related to business goal 'correct healthcare', which means that the patient should receive the healthcare he and she is entitled to. In this context the goal 'reliable information' is related to mentioned earlier responsibility that emphasizes organisational accountability to its partners and clients i.e. patients in hospital settings. Finally, the third CIA-concept, availability, has the same meaning as the main goal 'Available information'. Both objectives aim to make sure that information is accessible irrespective of time or place. This goal is also related to business goal 'correct healthcare', but also to the business goal 'effective healthcare' and by these two business goals 'available information' is related to organisational responsibility to its stakeholders. But, the CIA-triad fails to cover the other ISS-goals we found in the formal documents from Karlskoga hospital. These are 'Follow information security 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 information security 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, and not only trace the individuals that produce the information. This goal contributes to business goals: 'correct healthcare' and 'effective healthcare' and in the end is related to organisations responsibilities to its stakeholders.

Remaining main ISS goals found in the study 'Follow ISS laws, rules, and standards,' 'Standardized information' and 'Informed patients and/or family' are related to business gaols 'efficient healthcare' and 'empowered patients and can be related the broader interpretation of responsibility (Dhillon, 2007). The goals we have identified show that the hospital has responsibilities to other actors and the responsibilities should be considered in deciding policies and guidelines related to information handling and information security. We consider it important that the information security goals are associated to the business context in order to maintain the integrity of the organisation. 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

Conclusion

The purpose of this paper was to analyse information security goals at a Swedish hospital, and relate them to the traditional objectives of ISS – the CIA-triad (confidentiality, integrity and availability) used in information security standards. 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 organisation or type of organisation. Hence, the CIA-triad fails to cover organisational specific information security aspects of a hospital. Seven main information security 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. 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.

The study shows that special information security goals are needed in hospital settings and just applying CIA does not satisfy all hospitals needs related to information security. It seems to be more fruitful to start with organisational responsibilities to its stakeholders and with business goals to find specific information security goals for an organisation. The findings are in line with the ongoing discussion about objectives for security in the wider perspective where social and organisational aspects are considered.

References

Anderson, J. (2002). Why we need a new definition of information security. *Computer & Security, 22*(4), 308-313.

Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management, 15*(5/6), 337-346.

Datainspektionen. (2005). *Ökad tillgänglighet till patientuppgifter* (No. 2005:1).

Dhillon, G. (1997). *Managing information system security.*London: Macmillan.

Dhillon, G. (2007). *Principles of information systems security: Text and cases.*Hoboken, NJ: Wiley Inc.

Dhillon, G., & Backhouse, J. (2000). Information security management in the new millenium. *Communication of the ACM, 43*(125).

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal, 16*(3), 293-314.

Freeman, E. H. (2007). Holistic information security: Iso 27001 and due care. *Information Systems Security*(16), 291-294.

Gerber, M., & von Solms, R. (2005). Management of risk in the information age. *Computers & Security, 24*, 16-30.

Harris, S. (2002). *Cissp all-in-one certification exam guide.*New York, USA: McGraw-Hill/Osborne.

Hedström, K. (2007). The values of it in elderly care. *Information Technology & People, 1*(72-84).

ISO/IEC 17799. (2005). Iso/iec 27002:2005 information technology - security technigues - code of practice for information security management.International Organization for Standarisation (ISO), www.iso.org.

McFadzean, E., Ezingeard, J.-N., & Birchall, D. (2006). Anchoring information security governance research: Sociological groundings and future directions. *Journal of Information System Security, 2*(3).

Moulton, R., & Coles, R. S. (2003). Applying information security governance. *Computers and Security, 22*(7), 580-584.

Oscarson, P. (2007). *Actual and percived information systems security.* Linköping Univeristy, Linköping, Sweden.

Siponen, M., & Baskerville, R. (2001). A new paradigm for adding security into is development methods. In J. Eloff, L. Labuschange, R. Solms & G. Dhillon (Eds.), *Advances in information security management & small systems security* (pp. 99-111). Boston: Kluwer Academic Publishers.

Sveriges kommuner och landsting, Socialdepartementet, Läkemedelsverket, AB, A., & Carelink. (2006). Nationell it-strategi för vård och omsorg:Socialdepartementet.

Thomson, K.-L., & von Solms, R. (2006). Towards an information security competence maturity model. *Computer Fraud & Security*, 11-14.

Thomson, K. L., von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud and Security*(10), 7-11.

Tormpeter, C. M., & Eloff, J. (2001). A fremework for implementation of socio-ethical controls in infomration security. *Computers & Security, 20*(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, 20*(2), 136-143.

Von Solms, B. (2000). Information security - the third wave? *Computers & Security, 19*, 615-620.

von Solms, B. (2006). Information security - the fourth wave. *Computers & Security, 25*, 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). *Modeling 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.