HealthManagement
Promoting Management and Leadership

Volume 11, Issue 2 / 2009 - Management

Managing Information Systems Security

Compliance Between Users and Managers

Users are often viewed as an obstacle, a problem, within information systems security. One problem often raised is the users' low awareness of information systems security (ISS) regulations. The purpose of ISS is to, through technical, administrative or managerial means, protect an organisation's information resources. Having good ISS measures is important in hospitals, both for patient security and patient privacy. ISS routines that do not work can lead to maltreatments due to incorrect information, or disclosure of sensitive information to un autho rised people. To analyse how users comply with ISS regulations and policies is important if we want to gain an understanding of the impact, and use, of ISS measures. It is equally important to identify whether users have developed their own routines to deal with security risks.

The results in this article are based on a compliance study at the surgery clinic and medical clinic at Karlskoga hospital – a small Swedish county hospital in central Sweden. The hospital serves approximately 90 000 citizens, and is located in the County of Örebro, responsible for the healthcare of its 274 000 inhabitants. The two clinics were chosen as they handle a large amount of patients, and complement each other in terms of ICT (information and communication technology) use. The surgery has yet to introduce electronic health records (EHR), while the medical clinic regularly uses EHRs. Apart from the medical records, the clinics also handle patient information for e.g., operation planning or discharge notes. The study focused on the users' handling of patient information and whether they followed ISS regulations or not.

Regulations and policies regarding ISS measures were identified by analysing hospital- wide, as well as clinic specific formal routines found in documents as well as through interviews with regulators (e.g., quality manager, ISS manager).

Users' ISS measures were identified through interviews with nurses, doctors, and administrators at each clinic. The interviews were further contrasted and complemented with observations of how the users work with patient information.

ISS Regulations in Practice

We identified three compliance areas. The first is when users follow the ISS measures put forward in formal regulations and policies, the second is when users' actions are in conflict with formal regulations and policies, and the third and final compliance area illustrates instances when users have developed their own ISS measures. These three areas demonstrate that users are aware of formal ISS regulations and policies, but that they sometimes choose, consciously or unconsciously, to deviate from them, and that there are important ISS issues that the formal regulations and policies fail to cover.

Users Follow Formal Regulations and Policies

We found that users normally follow formal ISS regulations and policies. There was high compliance with formal measures regarding rules describing how to maximise the integrity of patient information, the availability of patient information and confidentiality of patient information. A formal routine to ensure the integrity, the correctness, of patient information can be formulated as 'test results must be signed before they are put into the medical journal.' Observations of the daily routines at the medical clinic confirmed that the users followed this routine. One rule describing how to make information available is written as 'everything that is of importance has to be documented in the medical journal.' We found many user actions following this specific rule. To ensure confidentiality of patient information was also an important formal ISS measure. One such routine was to make sure that sensitive patient information, such as copies of the medical journal, was destroyed, and not thrown in the bin, risking disclosure to unauthorised people. Interviews as well as observations confirmed that this rule was followed by users in the clinics.

Users in Conflict with Formal Regulations and Policies

Users sometimes failed to follow the formal regulations and policies. It is common with conflicts between formal rules aiming at maximising integrity of patient information and the nurses' and doctors' efforts to spend as much time as possible with the patients. The chief physicians were for instance exempted from signing dictates, which is a specific requirement in several formal documents regulating the ISS routines, as they prioritised meetings with the patients. Another conflict area is between formal regulations and policies regarding maximising confidentiality of patient information, and doctors and nurses need for patient information that is easily available. ISS measures regarding confidentiality of patient information is often written in the formal regulations and policies as 'medical journals shall be handled in a way that prevents unauthorised people from accessing them.' Even though this is acknowledged as a very important rule by doctors and nurses, they sometimes deviate from this rule in order to make their daily work more efficient. It is, for instance, quite common that medical journals are placed in easy accessible, but not very secure, places in order to make it quicker and easier for the doctor to access the medical journals before a patient consultation.

Users Develop Their Own ISS Measure

Our last compliance area describes when users develop ISS measures that formal policies and regulations fail to cover. Almost always, this concerns ISS measures regarding the availability of patient information. It is very important for doctors and nurses to have easy access to patient information. This means patient information must be well-arranged. The users arrange for instance the medical journals in alphabetical order. 'The medical journals are arranged in alphabetical order. It is important that the medical journals are in order. Otherwise it is difficult to find the information you

need.' Another important thing is to have complete patient information before the doctor's consultation with the patient. 'The day before [a patient consultation] we go through all the medical journals, make sure all journals are there, all referrals, and all test results.'

Conclusion

Our work at Karlskoga hospital has shown us that users are, contrary the prevalent view, aware about the importance of

ISS, and that doctors, nurses and administrators normally follow the prescribed ISS measures. What surprised us was, however, how little the formal rules and regulations addressed the users' need for easy and timely available patient information. The need for available patient information was often stronger then the urge to follow prescribed rules, which sometimes made them deviate from the formal regulations. Another observation was that the formal rules and regulations were focused mainly on electronic patient information, which made the formal view on ISS and the need for ISS measures very limited as they failed to address information that is handled manually. An exception to this was the manual medical records that were regulated in a separate document. ISS is much more than only electronic information, and a large part of the patient information is handled manually, which makes it important that formal rules and regulations cover manual patient information as well.

It is important to acknowledge, and be aware of users' compliance with ISS regulations and policies, in order to develop the secure management of patient information. Hospital managers need to understand doctors' and nurses' priorities and work practices. Our study has for instance shown the need for timely and efficiently available patient information in healthcare institutions. This illustrates the importance of including users' (here doctors and nurses) values in the management of ISS. If we fail to do so, there is a risk that we create ISS regulations and policies that are ignored or in the worst case, violated. Another risk is that we miss out important and central knowledge that users have and that could be of great value for creating measures for the protection of patient information.

Author:

Dr. Karin Hedström, Dr. Fredrik

Karlsson, Ella Kolkowska

Email: karen.hedstrom@oru.se

CIA Triad

The core principles of information systems security are widely known to be confidentiality, integrity and availability. This is known as the CIA triad.

Confidentiality

Information stored in the system, especially in the hospital environment must be kept confidential. Patient confidentiality must not be breached with the implementation of new and advanced information systems. Therefore creating appropriate levels of access to the in formation is important.

Integrity

Integrity in the context of information systems means preventing information from being modified without authorisation. This is particularly important regarding the accidental or malicious modification or deletion of files. For this reason processes must be appropriately tested before implementation to avoid errors, which in the hospital environment could have fatal consequences. Potential user mistakes should also be easily fixed.

Availability

The information stored in the system must be available when needed. The system must function properly at all times, giving its users access to the information they need within the appropriate timeframe while keeping in line with its security controls and coping with emergencies, power shortages etc. Availablility also means usability, is the system hard or easy to use?

The CIA triad is the point of reference for information systems security for both system design and management. However, it must be remembered that the triad is a limited model. In order to ensure successful security for your information systems the triad may be useful as a starting point but must be adapted accordingly. It does not, for example take into account the specifics of hospital information systems.

Published on : Mon, 20 Apr 2009