Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2005 Proceedings

Americas Conference on Information Systems (AMCIS)

2005

Secure Health Knowledge: Balancing Security, Privacy and Access

Ebrahim Randeree
SUNY Buffalo, er4@buffalo.edu

Secure Health Knowledge: Balancing Security, Privacy and Access

Ebrahim Randeree
SUNY Buffalo
er4@buffalo.edu

ABSTRACT

While decision analysis and treatment protocols have begun to move from health insurance companies into medical settings, secure knowledge management initiatives are being driven by HIPAA (Health Insurance Portability and Accountability Act) legislation. The needs of practitioners, researchers and students require that access be granted to pertinent patient data; balancing access and compliance in an environment that embraces new technological advances is difficult. HIPAA privacy and security guidelines curtailed the enthusiasm of open access with risk analysts placing an emphasis on risk-neutral behavior. This research in progress paper uses a case-based approach to address the role of security within a teaching institution. A research plan to test knowledge security and access is formulated.

Keywords

Security, Access, HIPAA, Knowledge

INTRODUCTION

As healthcare organizations increase their use of medical knowledge management systems, the embryonic concept of "secure knowledge management" has yet to be investigated. Knowledge management is increasingly becoming an integral function as organizations realize that competitiveness hinges on effective management of intellectual resources (Grover et al. 2001). Advances in technology have fostered the use of data warehouses and knowledge repositories, creating new challenges for security of patient information. If medical knowledge systems drive improved patient care and positive outcomes, then improving accessibility should be a key component (Bailey 2003). However, the passage of HIPAA has focused health care entities on the security and privacy of individually identifiable health information (IIHI). The trend of increased accessibility and facilitated patient access that was spurred by technological advances now has to be tempered by concerns of privacy and data security. Protection of knowledge has received little attention in the literature (Bloodgood et al. 2001).

The security component of HIPAA focuses attention on how health information is protected with respect to confidentiality, integrity and availability. The following sections will begin with an overview of the medical knowledge management system and then proceed to explain the security implementations and its effects. The complicated environment for this security and access will be discussed. Finally, the focus will turn to critical issues for future research in the area of secure medical knowledge management systems and the case-based analysis that is driving this research.

CASE STUDY – DESCRIPTION OF THE MEDICAL HEALTH SYSTEM

Systems designed to support knowledge may not appear to be radically different from other forms of information systems, but will be aimed towards enabling users to assign meaning to information and to capture their knowledge (Alavi et al. 2001). Recent research has shown that effective knowledge management requires a knowledge infrastructure (technology, culture, and structure), and a knowledge process architecture (acquisition, conversion, application, and protection) (Gold et al. 2001). The increased use of patient-care teams, medical reviews, and both internal and external audits, require special considerations for the sharing of knowledge. Information and data security considerations like those covered under HIPAA are not adequate for many reasons: the degree of collaboration or coupling is higher; sharing is based on trust; and current measures focus on database and data security (Damm et al. 2002).

Within the medical environment, the patient record is a primary focus of medical knowledge management. These records, which are stored in both hard copy and electronic format, include patients' medical history; medical findings such as examination results and radiographs; treatments planned by student care providers in conference with faculty supervisors; treatment progress and completion notes; and records of cash and insurance payments for treatments completed. Organizations that store and use medical records have to establish security measures to prevent unauthorized usage (Baumer et al. 2000). Adequate and appropriate access to the patient record is a necessary component of medical knowledge management, so privacy and security concerns must be balanced against the needs of students, faculty, and medical staff in providing optimum patient care. Providing quality care is a function of improved access to information and the sharing of information with relevant health care professionals in a timely manner; the consequences of increasing the breadth of available knowledge have yet to be explored (Alavi et al. 1999).

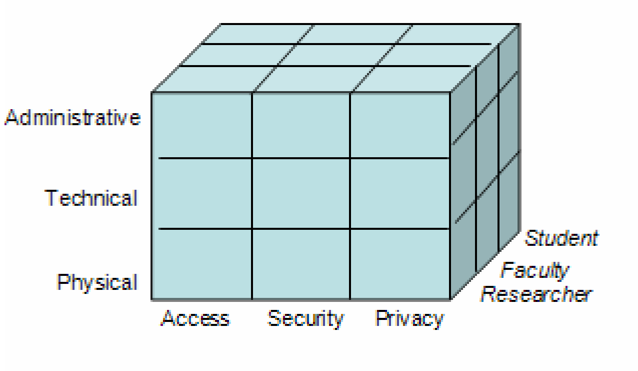

Figure 1 – Research Environment For The Case Study

DESCRIPTION OF THE ENVIRONMENT

The HIPAA privacy rule requires that protected health information (PHI) – all individually identifiable health information, whether electronic, hard copy or spoken – be managed in a way that minimizes the risk of disclosing that information inappropriately (Walker 2002). The HIPAA security rule requires more specifically that all PHI in electronic form be stored and transmitted securely; security of other forms of PHI are considered to be covered adequately in the privacy rule (2003).

In our case study, the knowledge management system (KMS) is the central repository for electronic patient records. The KMS is a client-server database application that incorporates data relating to patient demographics, diagnosis and treatment planning, appointment scheduling, and financial obligations. Higher level functions that are not directly related to patient care include tracking student progress, evaluating student performance, and generating summary financial reports. The function of the entity's clinics is to educate students while providing quality patient care. This process requires access to the detailed patient record as well as collaborative interaction between students, faculty, patients and medical staff. It is essential to secure the entire medical knowledge process, including its electronic, physical, and human components. Figure 1 describes the intricacies of the environment – using administrative, technical and physical security solutions with various users within the organization (Users may also hold multiple roles).

Physical safeguards relate to the protection of physical computer systems, device, media, and facilities using access control through locks, keys, location, and disaster recovery plans. These are among the most straightforward safeguards. For example, the entity maintains PHI-containing servers in alarmed, environmentally controlled space and restricts student access to workstations that provide full access to the KMS outside of supervised clinic hours. Technical safeguards relate to processes that protect, control, and monitor access to PHI, including authentication, authorization, auditing, integrity, and secure (encrypted) transmission of data. Administrative safeguards include policies, procedures, and conduct of employees in relation to the protection of information (password policies, termination procedures, incident reporting). This section also assigns responsibilities and highlights the need for security awareness and training. The entity has numerous administrative procedures to protect PHI while allowing adequate access, and more are under development. For example, based on their defined role within the system, students can access the full-featured KMS only from designated workstations within our physical facility. From other computers, including those connected via a wireless network, a feature limited version that allows only appointment scheduling is available, minimizing access to PHI. This balances students' need to manage their medical activities with the entity's need to protect health information.

Restrictions on access to equipment containing PHI-related data, authorization- and role-based limitations on access to the medical information system, and mandatory privacy and security training are examples of some safeguards currently in place. Most of these safeguards, however, deal primarily with securing data and information, not knowledge, which is less tangible and therefore more difficult to secure. Under HIPAA, privacy defines the method which is used to display patient information and to whom it is displayed; security is defined as administrative procedural mechanism that ensures the safety of the information.

DISCUSSION AND FUTURE RESEARCH

In addressing the accessibility, security and privacy dimensions, research into secure medical knowledge management should explore theory (technology acceptance and adoption), external influences (government influences and new legislation that drives security regulations, knowledge sharing parameters, and user privileges), and technological advances (focusing on how the knowledge is being created, collected, and shared, and with whom; more specifically, how is knowledge being protected). Emerging threats to knowledge security are inevitable, requiring constant compliance and vigilance. Knowledge management systems will not appear radically different from existing IS, but will be extended toward helping the user assimilate information (Alavi et al. 1999). The creation of an organizational framework will entail a risk assessment, gap analysis, and compliance programs to ensure that the organization meets HIPAA guidelines.

Current Approach to Knowledge Security

The current approach to HIPAA security is to develop a comprehensive security program that extends beyond HIPAA compliance. The approach mimics efforts in the Federal sector to protect information.

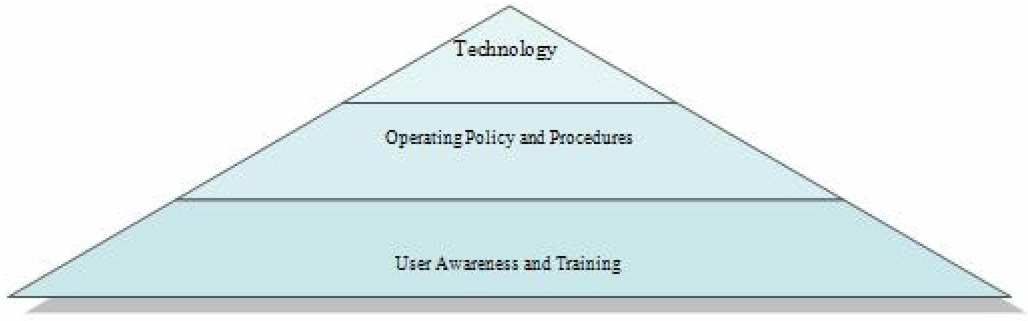

Figure 2 – Depth in Defense Pyramid (Schou et al. 2004)

Security and privacy of knowledge assets must be ensured without impeding access to the teaching and research functions within the entity. The methodology employed revolved around three facets:

- **Continuous Training:** Initial training of the three user groups was conducted on new policies and procedures under HIPAA (Privacy Rules specifically state that all of the covered entity's affected personnel must be trained). As part of a comprehensive HIPAA Compliance Program, all employees underwent a general HIPAA training ("HIPAA 101"), additional training was directed at high risk/ high priority areas (database controls, access points, medical records, etc). While technical and policy issues can easily be mandated and implemented, the weakest link in securing knowledge is securing the people with the knowledge (Smith 2003). User education and training is an integral part of the HIPAA implementation and compliance process; continuous training is implemented through semi-annual training, random compliance checks, periodic departmental audits, newsletters and bulletins, visible and alternating reminders, and repetition of guidelines. Within the organization, delivery of training is achieved through classroom training, computer self-study, and intranet programs. Online quizzes reinforce HIPAA compliance. The end goal is a cultural shift in attitudes that results in a HIPAA-compliant environment; the goal is to create a culture of security.

- **Continuous Risk Assessment:** Risk assessment for HIPAA focuses on four areas: physical assets, networking, software, business and medical processes (Jepsen 2003). Initial assessments of risks within the entity were followed with a gap analysis of current results with expected/HIPAA results. Procedures were enacted to comply with expected results. Each noncompliance was assigned a risk occurrence likelihood and impact level. The assessment is periodically performed at random intervals with subsets of the entire facility. Results are then compared to expected values and action is prescribed. Ongoing compliance within tolerance levels is acceptable. Non-compliance is followed with more training and review of procedures within the sample set.

- **Contingency Planning:** Planning for disruptions to compliance programs is essential for business continuity. Initial assessments of risks within the entity were followed with plans for dealing with an occurrence. In conjunction with training, plans need to be tested periodically to determine success rates. These plans will evolve as

HIPAA rules are interpreted on a federal level. Contingency planning documents “good faith efforts” to comply with HIPAA.

Issues for Research in Secure Knowledge Management

Current systems focus on data and information through access and encryption mechanisms. Current definitions of Knowledge Management Systems (KMS) are incomplete. They refer to a class of information systems applied to manage organizational knowledge; they are IT based systems developed to support and enhance the organizational processes of knowledge creation, storage/retrieval, transfer, and application (Alavi et al. 1999). The focus on security is missing. The entity is a repository of medical knowledge. Initially, such organizations must review the medical knowledge that currently resides within the facility in manuals, databases, reports, publications, and other artifacts. These entities must then be protected through security mechanisms. The abundance of patient related material is one of the biggest risks to organizations. Implementation procedures should focus on how the entity facility creates medical knowledge and the level of security that is sufficient for knowledge sharing. The next step involves establishing the level of authorization and access granted to different users. Secure knowledge management will include areas such as protecting the intellectual assets, secure collaboration, secure multimedia data and applications, secure semantic web as well as secure peer-to-peer computing. The nature of the knowledge being protected will determine the type of secure system that is implemented.

The Research Plan

The real challenge in security often lies with the weakest link, the people (Bresz 2004; Smith 2003; Vroom et al. 2004). A pilot study has shown that users are not compliant. This organization has students (with patient data access) at different exposure levels (4 years plus graduate programs) to security training. All users (including faculty and researchers) will be tested using surveys for retention of training and security knowledge creating a baseline score. With top management support, we can expect improved response rates. Data should reflect compliance with administrative and technical solutions and should reflect exposure to training sessions (we hope!). Users with more training are expected to demonstrate a cultural shift in their approach to security. Comparison to expected values will determine if further training will be needed; using follow-up surveys, we will create a model of security that includes administrative, technical and user solutions. This training model/solution combined with role-based security and a randomized testing protocol will be implemented on a wider basis within the regions medical entities and used as a benchmark for HIPAA compliance.

REFERENCES

1. "Health Insurance Reform: Security Standards, Final Rule," Federal Register, 2003, pp. 8334-8381.
2. Alavi, M., and Leidner, D.E. "Knowledge Management Systems: Issues, Challenges, and Benefits," *Communication of the Association for Information Systems* (1:7) 1999, pp 1-37.
3. Alavi, M., and Leidner, D.E. "Review: Knowledge management and knowledge management systems: Conceptual foundations and research issues," *MIS Quarterly* (25:1) 2001, pp 107-136.
4. Bailey, C. "Using Knowledge Management to make health systems work," *Bulletin of the World Health Organization* (82:11) 2003, p 777.
5. Baumer, D., Earp, J.B., and Payton, F.C. "Privacy of medical records: IT implications of HIPAA," *Computers and Society* (30:4) 2000, pp 40-47.
6. Bloodgood, J.M., and Salisbury, W.D. "Understanding the influence of organizational change strategies on information technology and knowledge management strategies," *Decision Support Systems* (31:1) 2001, pp 55-69.
7. Bresz, F.P. "People-Often the Weakest Link in Security, But One of the Best Places to Start," *Journal of Health Care Compliance* (6:4) 2004, pp 57-60.
8. Damm, D., and Schindler, M. "Security issues of a knowledge medium for distributed project work," *International Journal of Project Management* (20:1) 2002, pp 37-47.
9. Gold, A.H., Malhotra, A., and Segars, A.H. "Knowledge management: An organizational capabilities perspective," *Journal of Management Information Systems* (18:1) 2001, pp 185-214.
10. Grover, V., and Davenport, T.H. "General perspectives on knowledge management: Fostering a research agenda," *Journal of Management Information Systems* (18:1) 2001, pp 5-21.
11. Jepsen, T. "IT in healthcare: progress report," *IEEE IT Pro* (5:1) 2003, pp 8-14.

12. Liebeskind, J.P. "Knowledge, strategy, and the theory of the firm," *Strategic Management Journal* (17) 1996, pp 93-107.
13. Schlienger, T., and Teufel, S. "Analyzing information security culture: increased trust by an appropriate information security culture," Database and Expeprt Systems Applications, Fribourg, Guatemala, 2003, pp. 405-409.
14. Schou, C.D., and Trimmer, K.J. "Information Assurance and Security," *Journal of Organizational and End User Computing*. (16:3) 2004, pp 1-8.
15. Smith, S.W. "Humans in the loop: human-computer interaction and security," *IEEE Security & Privacy* (1:3) 2003, pp 75-79.
16. Vroom, C., and Solms, R.v. "Towards information security behavioural compliance," *Computers & Security* (23:3) 2004, pp 191-198.
17. Walker, R.J. "A HIPAA Strategy for Dental Schools," *Journal of Dental Education* (66:5) 2002, pp 624-633.