



IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax: 717/533-8661; URL-<http://www.idea-group.com>

ITB10374

Chapter XXIII

Secure Knowledge Management for Healthcare Organizations

Darren Mundy, University of Hull, UK

David W. Chadwick, University of Salford, UK

ABSTRACT

As the healthcare industry enters the era of knowledge management it must place security at the foundation of the transition. Risks are pervasive to every aspect of information and knowledge management. Without secure practices that seek to avoid or mitigate the effects of these risks, how can healthcare organisations ensure that knowledge is captured, stored, distributed, used, destroyed and restored securely? In an age where risks and security threats are ever-increasing, secure knowledge management is an essential business practice. The cost of security breaches in a healthcare context can range from the unauthorized access of confidential information to the potential loss or unauthorized modification of patient information leading to patient injury. In this chapter the authors highlight different approaches to minimising these risks, based on the concepts of authentication, authorization, data integrity, availability and confidentiality. Security mechanisms have to be in-depth, rather like the layers of an onion, and security procedures have to be dynamic, due to the continually changing environment. For example, in the past, cryptographic algorithms that were proven to be safe, e.g., 56 bit key DES, have succumbed to advanced computer

This chapter appears in the book, *Creating Knowledge-Based Healthcare Organizations*, edited by Nilmini Wickramasinghe, Jatinder N.D. Gupta and Sushil Sharma. Copyright © 2005, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

power or more sophisticated attacks, and have had to be replaced with more powerful alternatives. The authors present a model for ensuring dynamic secure knowledge management and demonstrate through the use of case studies, that if each of the security layers are covered, then we can be reasonably sure of the strength of our system's security.

THE CONTEXT FOR SECURE KNOWLEDGE MANAGEMENT

Knowledge is intangible, expensive to obtain, easy to lose and invaluable to organizational success. An organization's knowledge can also be easy to view, steal, manipulate and delete. In the physical world knowledge is protected by structures such as non-disclosure agreements, filing cabinets and shredding machines. In the digital world the same kind of mechanisms are required to ensure our knowledge is well protected.

Security threats to organizational data are increasing exponentially both within organizational boundaries and externally. According to the respected CSI/FBI Computer Crime and Security Survey 2002 (Power, 2002), the largest majority of attacks on computer networks are internal. In this chapter initially we present a conceptual model for ensuring secure knowledge management in healthcare. Then we introduce key security technologies which can be used to implement components of the model, as well as providing background information on how these components have traditionally been implemented within IT systems. Finally we provide case studies of recent implementations that illustrate use of the model. We believe this will convince the reader that security is a necessity in the implementation of Knowledge Management Systems (KMS).

ENSURING SECURE KNOWLEDGE MANAGEMENT IN HEALTHCARE

A model for ensuring secure knowledge management in healthcare is shown in Figure 1.

- *authentication*: (1) Security measure designed to establish the validity of a transmission, message, or originator; (2) a means of verifying an individual's eligibility to receive specific categories of information (NIS, 1992) (see "Authentication Mechanisms");
- *authorization*: (1) The rights granted to a user to access, read, modify, insert, or delete certain data, or to execute certain programs; (2) access rights granted to a user, program, or process (NIS, 1992) (see "Authorization Mechanisms");
- *data security (privacy)*: (The) protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure (NIS, 1992);
- *data integrity*: 1. (The) condition that exists when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed (NIS, 1992) (see "Data Security and Integrity during Transfer");

14 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/secure-knowledge-management-healthcare-organizations/7244

Related Content

Improving Assistive Technology Training in Teacher Education Programs: The Iowa Model

James R. Stachowiak and Noel Estrada-Hernández (2010). *Handbook of Research on Human Cognition and Assistive Technology: Design, Accessibility and Transdisciplinary Perspectives* (pp. 286-298).

www.irma-international.org/chapter/improving-assistive-technology-training-teacher/42843

Bibliographic Analysis of Medication Adherence and Use of Reminders

Saibal Kumar Saha (2022). *International Journal of Reliable and Quality E-Healthcare* (pp. 1-13).

www.irma-international.org/article/bibliographic-analysis-of-medication-adherence-and-use-of-reminders/296692

Exploring Region of Interest (ROI) to Support Quality of Service in Unreliable Wireless Electronic Healthcare Communications

Wei Wang, Min Zhao, Honggang Wang and Kun Hua (2012). *International Journal of Healthcare Information Systems and Informatics* (pp. 1-12).

www.irma-international.org/article/exploring-region-interest-roi-support/75146

On Performance of Big Data Storage on Cloud Mechanics in Mobile Digital Healthcare

Abhilasha Rangra and Vivek Kumar Sehgal (2021). *International Journal of E-Health and Medical Communications* (pp. 36-49).

www.irma-international.org/article/on-performance-of-big-data-storage-on-cloud-mechanics-in-mobile-digital-healthcare/277445

Diffusion

Roy Rada (2008). *Information Systems and Healthcare Enterprises* (pp. 322-336).

www.irma-international.org/chapter/diffusion/23389