Decision Support Systems xxx (2012) xxx–xxx

Contents lists available at SciVerse ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss

A decision methodology for managing operational efficiency and information disclosure risk in healthcare processes

Xue Bai *, Ram Gopal, Manuel Nunez, Dmitry Zhdanov

Department of Operations and Information Management, School of Business, University of Connecticut, Storrs, CT 06269, USA

ARTICLE INFO

Available online xxxx

Keywords:
Information disclosure
Risk
Workflow efficiency
Control
Healthcare processes
Optimization

ABSTRACT

This paper addresses two critical challenges faced by healthcare organizations: significant personnel shortages and mandates to safeguard patient safety and information security. We develop a two-stage decision making methodology to optimize the healthcare workflow task assignments and mitigate information disclosure risks. While the first stage throughput optimization formulation maximizes operational efficiencies, it can expose organizations to information disclosure risks that can be exploited to violate patient safety and information security. To address the ensuing privacy and fraud concerns we define task-based conflict sets to assess disclosure risks with optimal task assignments. In the second stage of the solution methodology, various security control strategies – task based and employee based – are incorporated into a decision support model to help decision makers to effectively manage and achieve workflow efficiency and meet information security requirements. For practical settings where certain parameters are not obtainable or the problem is computationally intractable, we provide a sequential-decision approach that could yield approximate partial solutions. We conduct an extensive computational analysis of a clinical workflow process to illustrate the practical benefits of the proposed methodology.

1. Introduction

As healthcare costs continue to skyrocket, healthcare organizations are faced with the constant challenge of operating at reduced costs while delivering good quality of care and protecting patient privacy [1,30,31]. However, the ability of these organizations to deliver effective and efficient patient care is currently hindered by two major factors: the current and growing shortage of healthcare professionals and the patient privacy concerns. On the one hand, staffing shortages across healthcare job types have caused emergency department overcrowding, reduced number of staffed beds to serve patients, delayed discharge and increased length of stay for patients, and decreased staff and patient satisfaction [1]. On the other hand, organizations are mandated to comply with a plethora of rules and regulations to ensure patient privacy [30,31]. Such rules and regulations are a natural consequence of concerns about healthcare organizations that routinely collect, manage and use sensitive personal, medical, and financial data on patients. While access to such data is crucial to deliver quality care and conduct clinical research, they may also be exploited for profit and enable a variety of criminal activities. For example, a former UCLA employee pleaded guilty to selling medical data of celebrities to tabloids [39]. In a series of related investigations, it was discovered that records of over 1000 patients were accessed inappropriately since 2003; 165 hospital employees were disciplined. Motivations for private data snooping may go beyond mere curiosity or selling data to tabloids. By collecting pieces of information about a person, a potential attacker can create a comprehensive profile of the target and use it later for identity theft, blackmail or other adverse activities.

Regulations such as HIPAA (2002) [30] and HITECH (2009) [31] require healthcare organizations to implement policies and procedures to prevent and detect security violations related to patient safety and privacy. Such initiatives are in themselves not revenue generating activities but rather an additional cost for organizations. In light of staffing shortage, budget constraints, and an avalanche of evolving regulatory compliance requirements, healthcare organizations are driven to design and improve the operation efficiency and information security in their workflow systems.

Despite large and diverse research on healthcare processes and information security, there is dearth of research addressing healthcare processes with the objective of achieving both the operational efficiency and meeting information security requirements. Research in healthcare informatics has focused on developing security mechanisms for electronic clinical record systems, while research in information security has focused on developing various technologies at microdata level or database access mechanisms to limit the disclosure of sensitive data [9,14–16,18,21,25,40]. One of the key challenges in the design of healthcare processes and other service-oriented environments is to achieve the goal of both providing efficient care and

* Corresponding author.
E-mail addresses: xue.bai@business.uconn.edu (X. Bai), ram.gopal@business.uconn.edu (R. Gopal), manuel.nunez@business.uconn.edu (M. Nunez), dmitry.zhdanov@business.uconn.edu (D. Zhdanov).

0167-9236/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.dss.2012.10.046

securing privacy information adequately [38,55]. We recognize this challenge and explicitly address it in our work.

In this paper, we propose a decision methodology that minimizes the disclosure risk via a workflow system with optimal efficiency and a viable and effective control scheme for preventing information disclosure. This methodology encompasses a two-stage optimization formulation. At the first stage, it finds optimal staffing solutions for a workflow, in terms of minimum throughput time. At the second stage, it then selects the best combination of task and employee control placements for each of the optimal staffing assignments obtained from the first stage, in terms of acceptable control cost. We show that solving the two-stage problem results in an efficient and reasonably secure staff strategy. For applications where model parameterization is practically infeasible or the problem is computationally intractable, we provide a sequential-decision methodology that could yield efficient staffing solutions with minimum disclosure risk. We use a clinical workflow process to illustrate our methodology.

2. Literature review

There is a general understanding that delivering quality health care is a complex endeavor which is highly dependent on utilizing information effectively [7]. Information systems that can help in medical and clinical decision making have been available for over three decades. While the usefulness of these systems is well understood, security concerns have been cited as one of the major barriers to their widespread adoption [36,37].

Research from health care informatics has focused on the development of sophisticated information and computer security mechanisms for electronic medical record systems (EMRS). Most commonly used technology in EMRS is the implementation of access management mechanisms such as role based access control [44]. However, role based access control has not been successful in complex environments like hospitals. As defining discreet and universal access roles is extremely difficult, hospital administrators rely on audit trails to detect intrusions of patient privacy [6]. Gallagher et al. [19] demonstrated one audit system for EHRs. This system partially reduced the burden on auditing personnel by giving users the ability to inspect the access data for their own record. Asaro and Ries [3] did a study to analyze the distribution of EHRs accessed by users. In this work, we provide a control strategy using the combinations of task monitoring and personnel monitoring control placements to reduce or completely prevent unauthorized data access.

The issue of providing proper information security configuration is a difficult one, since consequences of inadequate use of information or system failure can lead to severe, if not lethal, consequences. Several approaches are proposed to deal with this issue. A general set of guidelines are listed in the NIST 800-14 publication that specify eight generally acceptable principles and fourteen common IT security practices [26]. Some of the key principles are that computer security must support the mission of the organization, be cost-effective and be constrained by societal factors. All of these are true in the healthcare workflow environment and serve as the foundation for our analysis. In the healthcare setting, Gritzalis [23] provides a broad approach to the security of healthcare information systems by creating a baseline security policy. This policy is built based on the information system security profile including attitudes and awareness; experience; organizational environment; education and research; and mode of processing of the medical data. The healthcare field may be characterized by a distributed information processing environment utilizing heterogeneous systems. It is important to understand the information flows and protect the data at every step of the process. Common approaches used for data protection in the healthcare field include mobile agents [48,50] and middleware systems for ubiquitous data integration [41]. However, even with automated tasks, concerns over the exposure of private information still remain. Often, patient data is used in clinical research where knowledge of individual information is not essential for the research project, thus allowing for some sort of data distortion or access restriction mechanism to be enabled [9,11]. However, in the clinical workflow context where the individual data needs to be accessed, such solutions are not applicable. In our work, we propose a method for evaluating and mitigating information disclosure risk via placement of monitoring controls.

In this context, monitoring controls can be assigned either at the task level (all instances of data access in a specific task are recorded, regardless of the employee) or at the employee level (specific employees are monitored in all of their tasks). While both of these approaches are possible, they are not devoid of some problems. In case of employee monitoring, while organizations may expect benefits such as prevention of resource misuse and reduction of corporate liability due to misbehavior of its employees [2], there may also be substantial drawbacks to it. For instance, employee monitoring may have a negative impact on morale, encourage a negative management style, and even cause economic loss due to decreased productivity of employees and managers alike [2]. In addition, there is a variety of employee behaviors with regard to information security that may be hard to categorize before those become manageable [47]. These and other concerns prompt researchers to question the effectiveness of employee audit as a viable tool for behavioral compliance with information security requirements [51].

Typical task-centered controls include technical solutions such as access control, audit tools and intrusion detection systems. Access control tools are preventative solutions that are designed to stop unauthorized access and data disclosure before it happens. There are multiple solutions such as access control lists (ACL) and role-based access control (RBAC), among others (please see [49] for a detailed review). However in many cases these controls are too rigid for modern day clinical workflows and can be effective only in relatively simple scenarios [10]. In addition, in some circumstances, such as medical emergencies, these controls may have to be overridden, leaving open opportunities for the malicious activities.

One of the prominent ways to make RBAC useful in practice is known as role engineering [12,13,46]. The process of role engineering is essentially requirement engineering and has important concepts such as static and dynamic separation of duties. Static separation of duties implies hard restrictions of data access by a role at the design level, while dynamic separation of duties is enforced at runtime and is based on the particular data instances. In our work, we explore the effects of these principles via authorization rules and conflict sets.

Role engineering is a broad and active area of research and the reader can find many details in [22]. Our focus here is on the ideas of role engineering with regard to security and privacy. While traditional RBAC approach is built around the basic elements of the users, roles and permissions, these elements are not necessary to represent privacy authorization rules. They need to be amended with the elements of purposes, conditions and obligations of using private data [29,34]. We implicitly address these issues via the analysis of risk exposure of private data. Specifically in healthcare, role engineering started with the definitions of basic roles – such as patient, doctor, researcher – by Barkley [5]. Subsequent work explored many modifications of RBAC based on the authentication context [32], doctor location [27], principle of explicit denial of access to some patient data [45] and inter-organizational differences in RBAC structure [33]. These works exemplify the broad scope of issues with what healthcare role engineering is dealing, and we think that our method can provide a solid decision support tool in making choices about healthcare roles. Even if the roles are well defined, there may be a need to override those constraints — such as in "controlled overriding" [52] or "break the glass" policy [17]. While these overrides trigger additional logging and audit routines, the risks of resulting privacy exposures are not discussed. Zhao and Johnson [54] provide