An Agile Enterprise Regulation Architecture for Health Information Security Management

Ying-Pei Chen, Ph.D. Cand.,¹ Sung-Huai Hsieh, Ph.D.,²
Po-Hsun Cheng, Ph.D.,³ Tsan-Nan Chien, Ph.D. Cand.,¹
Heng-Shuen Chen, M.D., Ph.D.,⁴⁻⁶ Jer-Junn Luh, Ph.D.,⁷
Jin-Shin Lai, M.D.,⁸ Feipei Lai, Ph.D.,⁹⁻¹²
and Sao-Jie Chen, Ph.D.^{1,12}

¹Graduate Institute of Electronic Engineering, National Taiwan University, Taipei, Taiwan.

²Department of Computer Science and Information Engineering, Providence University, Taichung, Taiwan.

Departments of ³Software Engineering and ⁴Medical Informatics, National Kaohsiung Normal University, Kaohsiung, Taiwan.

⁵Department of Family Medicine, National Taiwan University Hospital, Taipei, Taiwan.

⁶School of Medicine and ⁷School of Physical Therapy, National Taiwan University College of Medicine, Taipei, Taiwan.

⁸Department of Physical Medicine and Rehabilitation, National Taiwan University Hospital and College of Medicine, National Taiwan University, Taipei, Taiwan.

⁹Graduate Institute of Biomedical Electronics and Bioinformatics, National Taiwan University, Taipei, Taiwan.

¹⁰National Taiwan University Hospital, Taipei, Taiwan.
Departments of ¹¹Computer Science and Information Engineering and ¹²Electrical Engineering, National Taiwan University, Taipei, Taiwan.

Abstract

Information security management for healthcare enterprises is complex as well as mission critical. Information technology requests from clinical users are of such urgency that the information office

should do its best to achieve as many user requests as possible at a high service level using swift security policies. This research proposes the Agile Enterprise Regulation Architecture (AERA) of information security management for healthcare enterprises to implement as part of the electronic health record process. Survey outcomes and evidential experiences from a sample of medical center users proved that AERA encourages the information officials and enterprise administrators to overcome the challenges faced within an electronically equipped hospital.

Key words: business administration/economics, e-health, extreme environments, information management, policy

Introduction

Information security management for healthcare enterprises is quite complex and also mission critical. Information technology requests from clinical users are of such urgency that the information office should do its best to achieve as many of the user requests as possible at a high service level. Information requests have gradually decreased at 0.3% in the healthcare enterprise as surveyed in the National Taiwan University (NTU) Hospital from 2001 to 2007, where most of the requests have been registered in related information systems. *Figure 1* illustrates the number of requests and growth rates from January 2001 to December 2007. The figure shows that the growth rate of user requests has maintained its average level, even though the health information systems were restructured from 2005 to 2007 and users absorbed some of the requests themselves. Note that NTU Hospital owns 1,849 beds, serves 2,000,853 outpatients, and employs 5,226 professionals and employees in 2007.¹ Three-fifths of employees are system users.

However, it is difficult for the information office to ascertain whether these efforts effectively benefited the majority of the clinical

Fig. 1. Number of user requests and related growth rates per quarter from 2001 to 2007.

users at all. Along with the adoption of new information technologies to healthcare enterprise, such as the wireless network and the virtual private network, the access points for clinical information have been gradually diversified. To protect patients' privacy, it is compulsory for enterprise administrators to effectively implement some of the required information security management procedures.

In 1996, Sherwood² described a Sherwood Associate Limited Security Architecture (SALSA) model. The primary characteristic of the SALSA model is that everything must be derived from an analysis of the business requirements for security, especially those in which security has an enabling function through which new business opportunities can be developed and exploited. Further, Schekkerman³ collected and illustrated 14 leading frameworks for the design of an enterprise information architecture in 2006. Regrettably, the aforementioned frameworks cannot be remodeled to fit a healthcare enterprise, which will be the target of our research.

In 2008, Farn⁴ illustrated a new framework of information system security classification for e-Taiwan to reach the vision of "information and communication network resources fully used in an obstacle-free and secure environment by year 2008." The healthcare enterprise that is the subject of our research is one of the governmental units and has followed the national e-Taiwan policy for many years. Moreover, this

hospital had been defined as a Class A government organization in Taiwan and had passed the third-party Information Security Management System (ISMS) accreditation in 2007.

In addition, the hospital has attempted to achieve flexible and agile regulation architecture to adapt to organizational growth and the changing competitive environment for healthcare. Not only are standards and agility mutually compatible, both of these ideas are also key components of engineering disciplines.⁵ Experience has shown that standards mandated in inflexible policy, which do not account for real-world consideration, will ultimately fail.⁶ Consequently, regulations for healthcare enterprise should engage greater user experiences to reflect the actual user flows and requirements.

The U.S. Congress passed the Federal Information Security Management Act in 2002. Further, the National Institute of Standards and Technology (NIST) standards and guidelines were designed to allow for flexibility in Federal Information Security Management Act compliance and implementation. Comprehensively, NIST standards and guidelines support a bottom-up approach to security.⁷ The research presented here refers to the NIST standards and attempts to solve the following problems: how to achieve an Agile Enterprise Regulation Architecture (AERA) for health information security management; how to prove the effectiveness of our regulation exe-

cution outcomes and provide evidence that clinical users embrace our administrative security policies.

Enterprise Regulation Architecture

After reviewing several frameworks,^{2,3,8} it is hard to reconcile any of them with the research environment. For example, Schekkerman's³ book collected and analyzed at least 14 distinct frameworks from the United States and European Union in 2004. Some of them are suitable for e-Government, treasury, and defense departments but none of them can be directly as well as simply adopted in healthcare field. As the affiliated information frameworks are general, our development team set out to develop a specific framework for healthcare usage. Further, Ross-Lee and Weiser⁸ said that regulation after reform would react to outcomes rather than control the process of healthcare delivery. Their examination for clinical laboratory improvement amendments caused laboratories to close, thereby restricting access to healthcare.

Meanwhile, most of the healthcare regulation arguments might derive from some implicit factors of healthcare enterprise, such as organizational culture, colleague's computing capability, and system maturity. For example, a research fellow might want to install some research-oriented packages to his client computer but our regulations do not allow such an action because of virus protection. However, the fundamental regulations cannot persuade him to follow this minimum system limitation. Such a contention provides another viewpoint to our information system department and then our development team proposed the research-oriented matter to the Information Management Committee (IMC) to keep or revise related original regulations. Regulation definition is different and difficult to reconcile among healthcare enterprises in Taiwan.

This research proposed an AERA for information security management, allowing healthcare enterprises to plan and adopt the electronic health record (EHR) process. *Figure 2* illustrates the road map for AERA in our target enterprise and the following subsections delineate the integration perspectives, core services architecture, and integration implications, respectively.

It should be noted that we considered the relevant regulation processes before policy execution, as shown sequentially from the bottom to the top of the left-hand side in *Figure 2*. Meanwhile, our research evaluated the regulation execution performance step by step, using the points from left to right of the right-hand side in *Figure 2*. Fundamentally, we focus on our

management experiences and discuss the integration perspectives. To design the information maintenance management as well as continuously consider different perspectives, our information services are divided into three core services: hardware security, networking security, and software security. These three core services are bundled as a core service architecture. Such a core service architecture serves our users and produces at least two integration implications, that is, access control and data exchange.

INTEGRATION PERSPECTIVES

As indicated by the points on the left-hand side of *Figure 2*, our research targeted the central problems of healthcare privilege management. That is, our integration perspective focused on the law-related facet that includes the governmental laws, organizational regulations, and user obligations. Further, we evaluated the above four perspectives throughout the regulation execution period. These four perspectives are the enterprise, generic, portal, and service perspectives. Fundamentally, these four postconsideration perspectives are a virtual mapping of the three preconsideration perspectives.

For example, to expand our views on the integration perspectives and to satisfy the ISMS's audit of the e-Taiwan policy,⁴ we requested four information engineers to diligently perform the BS-7799 auditor certification and earned three BS-7799 professional licenses for the information security certificate in 2004 and 2005. Their backgrounds include networking administration, system administration, information education, and emergency information systems. Their

Fig. 2. Road map for agile enterprise regulation architecture.

domain know-how and security management feedback were gradually derived from the healthcare enterprise and used to refine our AERA. In addition, the information department provides information security training for the superintendent, chief information officer, information technology technicians, and general officials every year. Overall, we considered the integration perspectives prior to policy execution by following the law-oriented considerations and then reconsidered our regulations by following the implementation-oriented method's four integration perspectives.

CORE SERVICES ARCHITECTURE

On the basis of the considerations prior to policy execution of our integration perspectives and the information security "Defense-in-Depth" strategy of e-Taiwan,⁴ we considered and divided our health information services into three core services, that is, hardware security, networking security, and software security. All of these three core services were creatively built into our core service architecture and the related information security "Defense-in-Depth" strategy included the firewall, antivirus, intrusion detection system, and security operation center in our healthcare enterprise.

First, the hardware security focuses on personal computers, printers, operation room servers, databases, storage, and related information equipment. The networking security included at the very least the cable network, wireless network, firewall, and virtual private network. Additionally, the software security focuses on our in-house-developed applications, commercial software packages, and freeware applications. Correspondingly, the above three core services can be viewed in another perspective for postconsideration usage. That is, these services can be divided into policy view, user view, and data view. These three domains can additionally be mapped into organizational policy, user obligation, and data exchange, respectively.

In addition, our information department requires ISO-9001 service quality management every year and executes internal standardized operating procedures routinely. For instance, the information in *Figure 1* is extracted from one of these procedures, the computer functionality request sheets, and the related system functions are monitored by some special administrative flows.

INTEGRATION IMPLICATIONS

Beyond our preconsiderations for integration perspectives and core services architecture in *Figure 2*, we focused on access control and data exchange to consider the integration implications. On the other hand, we segmented the postconsiderations for integration implications into another four axes, that is, knowledge acquisition,

standard adoption, application integration, and security auditing. These relate on a one-to-one basis to each of the postconsideration integration perspectives. For example, knowledge acquisition is relevant to the enterprise domain.

Table 1 illustrates a multidimensional view of visiting staff (physicians) in the access control category. Hierarchically, our research apportioned a formal health procedure into five facets, that is, user, task, time, place, and route. We contemplated that a specific "user" executes a specific "task" at a specific "time" and "place" using a specific "route." As such, we can grant or abolish certain privileges after considering all the five facets.

The user facet can be separated into many different levels in the healthcare enterprise. For example, doctors can be separated by their level of experience, such as doctor for visiting staff, chief-of-resident, and resident. In addition, a medical center with teaching and research services may also include levels for interns, medical students, and research assistants. Other groups of users include nurses, technicians, clerks, vendors, and others.

Second, the task facet can be divided into either a query task or an update task. They can be further divided into many subtasks in terms of their functional complexity. For example, additional detail for the query task can be separated into the patient information query, the laboratory report query, the treatment status query, the scheduling status query, and the organizational infection report query.

Our security process splits the user time into either on-duty or off-duty. Both time periods comprise two distinctive execution localities, that is, on-campus and off-campus. When a user is located overseas but requires the use of computer resources, our policy allows override for a special situation and grants off-campus access privilege. Regardless of where a user is located, our enterprise supports a virtual private network for accessing enterprise computing resources. Users can access our computing environment through an office personal computer, office notebook, or personal notebook. The personal notebook is carried home by employees, whereas the notebook media access control (MAC) address and related information must be recorded by the information department before it is used inside the healthcare enterprise.

Table 1 is an example describing which users have the privilege to query patient information using an office personal computer or notebook on our medical campus. On the other hand, this privilege is abolished when the user travels outside the country, as there is no direct face-to-face patient diagnosis. Moreover, the National Health Insurance Bureau does not allow for such a modification and will abolish such a declaration in the future.

Table 1. An Example of Multidimensional Views

CATEGORY NAMES	USER	TASK	TIME	PLACE	ROUTE	PRIVILEGE
Access control	Doctor (VS)	Query	On-duty	On-campus	Official personal computer	Grant
					Official notebook	Grant
					Self notebook	Grant
				Off-campus	Virtual private network	Grant
			Off-duty	On-campus	Official personal computer	Grant
					Official notebook	Grant
					Self notebook	Grant
				Off-campus	Virtual private network	Grant
				Overseas	Virtual private network	Grant
		Update	On-duty	On-campus	Official personal computer	Grant
					Official notebook	Grant
					Self notebook	Grant
				Off-campus	Virtual private network	Grant
			Off-duty	On-campus	Official personal computer	Grant
					Official notebook	Grant
					Self notebook	Grant
				Off-campus	Virtual private network	Grant
				Overseas	Virtual private network	Abolish

Bylaws Integration

In 2001, the NTU Hospital, the subject of this research, created the Information and Communication Security Committee by the order of its supervising governmental department, Administration Yuan, Taiwan. This committee focused on information and communication security and proposed some basic regulations for hospital se-

curity management. For instance, it defined seven bylaws categories for further reference and development in December 2004. In October 2005, this committee was upgraded to the IMC for discussing and developing additional information technology and information security management issues. Further, we refined the previous seven bylaws categories and the related regulations. *Table 2*

Table 2. The Seven Major Regulation Categories and Related Regulations

CATEGORY NAMES	REG. NO.	REGULATIONS	PRECONSIDERATION	POSTCONSIDERATION
Organizational policy (OP)	OP.1	Information security preventive measures	GL, OP, UO	ED, GD
	OP.2	Information security management points	GL, OP, UO	ED, GD, SD
	OP.3	System crash emergent processing guideline	OP, UO, HS, NS, SS	ED, GD, SD
User obligation (UO)	UO.1	Password operating rules	OP, UO	SD, PD
	UO.2	Official PC authority points	OP, UO	SD, PD
	UO.3	Official E-mail utilization points	OP, UO	SD
Hardware security (HS)	HS.1	IT equipment management regulation	OP, HS	PV, UV
	HS.2	Computer classroom regulation	OP, UO, HS	PV, UV
	HS.3	IT environment management points	OP, HS	PV, UV
	HS.4	PC utilization classification guideline	OP, HS	PV, UV
	HS.5	Information room management guideline	OP, HS	PV
	HS.6	Vendor maintenance management guideline	OP, HS	PV, UV, DV
	HS.7	Vendor recognizance	OP, HS	PV, UV
Networking security (NS)	NS.1	Network utilization management points	OP, NS	PV, UV, DV
	NS.2	Network utilization recognizance	OP, NS	PV, UV
	NS.3	Virtual private network management points	OP, UO, NS	PV, UV, DV
Software security (SS)	SS.1	Software development and maintenance regulation	OP, SS, DE, AC	PV, DV
	SS.2	Web site setup operating rules	OP, UO, SS, DE, AC	PV, UV, DV
	SS.3	PACS user privilege regulation	OP, UO, SS, DE, AC	PV, UV, DV
	SS.4	HIS user privilege regulation	OP, UO, SS, DE, AC	PV, UV, DV
Access control (AC)	AC.1	Information security management constrain	GL, OP, DE, AC	KA, StdA, AI, SecA
	AC.2	Database account management regulation	OP, HS, NS, SS, AC	KA, StdA, AI, SecA

continued →

Table 2. The Seven Major Regulation Categories and Related Regulations (*continued*)

CATEGORY NAMES	REG. NO.	REGULATIONS	PRECONSIDERATION	POSTCONSIDERATION
Data exchange (DE)	DE.1	Data request guideline	GL, OP, UO, DE, AC	KA, StdA, SecA
	DE.2	Data request recognizance	GL, OP, UO, DE, AC	KA
	DE.3	EHR request management regulation	GL, OP, UO, DE, AC	KA, StdA, SecA
	DE.4	EHR request guideline for teaching/research	GL, OP, UO, DE, AC	KA, SecA
	DE.5	Official PC installing packages guideline	OP, AC	AI, SecA

AI, application integration; DV, data view; ED, enterprise domain; EHR, electronic health record; GD, generic domain; GL, governmental laws; HIS, health information system; IT, information technology; KA, knowledge acquisition; PACS, picture archiving and communication system; PC, personal computer; PD, portal domain; PV, policy view; StdA, standard adoption; SecA, security auditing; SD, service domain; UV, user view.

illustrates the seven major regulation categories in the medical center.

QUESTIONNAIRE SYSTEM

Actually, our development team customized the security regulation architecture for our new hospital information systems that had been implemented since 2004. Therefore, the “users” at least include the colleagues who utilize the new developed systems for their daily tasks in our healthcare enterprise. Also, it is necessary that the new users hired by our enterprise, who need to apply for a new account and to utilize our enterprise computing resources, are authorized by their managers and information systems department.

The access privilege is dependent on the user's management level. Also, a single user might have different access rights depending upon current location. For example, a physician owns the full privilege to update his patient's EHRs inside our healthcare enterprise environment. However, he cannot update the same patient's records while he is traveling outside the country.

Most of the information security regulations are revised from old systems and adapted for new applications. As the new applications adopt the latest information technologies, related user-computer interaction interfaces are changed. It is a helpful to

Fig. 3. Question B5 statistical graph for both outpatient and inpatient information systems in 2007.

clarify the business processes for reengineering systems in the healthcare enterprise. The new information technology adoption is requested from most of the users, such as the Web-based applications, service-oriented architecture,⁹ single-sign-on portal, and the like. Our development team as well implemented a conceptual persistent healthcare quality improvement process¹⁰ for software development managers to review our execution outcomes continuously. As our proposed process is an iterative approach, we named it as an agile framework.

That is, our information system department attempts to utilize a questionnaire mechanism to show indirectly whether our regulation formulation is acceptable and effective in our healthcare enterprise. The questionnaire might effectively collect more voices from our implicit colleagues than personal interview. Most Oriental people are timid and rarely convey their implicit expressions in public places. Accordingly, we believe that an appropriate questionnaire mechanism is more opportune in Eastern countries than Western ones.^{11,12}

The sample size of our survey covers all of the colleagues who utilize our developed systems. To simplify the survey difficulty and expedite the survey efficiency, our software development team created a survey system to gather all the questionnaire answers online. Our survey questionnaire contained 34 questions and utilized a five-point Likert scale. Approximately 7% of the system users attended our survey.

MAJOR EXECUTION LINE

The major execution line of our regulation execution follows our reconsideration and postconsideration axes, which were mentioned in the previous section. That is, our IMC considered the governmental laws, organizational policy, and user obligation perspectives through the regulation's discussion and defining periods and then considered the enterprise, generic, portal, and service perspectives during the regulation execution and evaluation periods. For example, the OP.2 information security management points referred to some of the governmental laws, such as the electronic signature law and the personal data protection law. Also, OP.2 is the main regulation in our enterprise that is referred by all the other regulations.

Survey outcomes from the medical center users proved that our proposed architecture encourages the information office and enterprise administrators to adopt the proposed EHR. The surveys for both the

outpatient information system (OIS) and inpatient information system (IIS) were prepared using the same questions in separate questionnaires.

For example, question B5 (I feel our new information system implementation follows obvious regulations) in *Figure 3* illustrates that most of our OIS users feel that the enterprise regulations are clearly defined. The sum of grade 4 and grade 5 for OIS oscillated from 34.98% to 34.15%, and finally increased to 47.54% within 1 year. However, on the other hand, the percentage of IIS users who were not satisfied with the enterprise regulations suggests that our IMC should attempt to find and refine the unsatisfactory points of the regulations. The sum of grade 4 and grade 5 for IIS changed from 38.96% to 34.38%, and finally to 36.07%.

Similarly, the statistical graph for question B7 (I feel our new information system is more secure than ever) in *Figure 4* shows that the sums of grade 4 and grade 5 for OIS and IIS changed from 40.36% to 39.02%, and finally to 42.62% and from 33.76% to 21.88%, and

Fig. 4. Question B7 statistical graph for both outpatient and inpatient information systems in 2007.

finally to 24.59%, respectively. Further, most of the users have the same percentage of grade 3 for both OIS and IIS. That is, the average percentages of grade 3 are above 44.50% and 53.25% for OIS and IIS, respectively. The evidence proves that users trust our information system and encourage our IMC and information management center to continuously refine our working processes and related regulations.

Discussion and Future Works

Several arguments have been considered by the healthcare enterprise colleagues. These include how to trust other colleagues, the minimum number of regulations, and setting up one channel for accessing all materials. In addition, it must be considered what the next step is for the healthcare enterprise. The following subsections consider these arguments.

TRUST YOUR COLLEAGUES FIRST

As the first sentence of the famous Chinese Trimetric Classic said "Men at their birth are naturally good. Their natures are much the same; their habits become widely different."¹³ The major tenet of our enterprise regulations is to trust our colleagues at first. Such a belief will obviously decrease the number of regulations and change the controversial subject definition of all related regulations. That is, we believe that it is the wisest choice for us to return to human nature. Therefore, our IMC defines and also refines the regulations to be based on such a confident belief in promoting the related contents.

THE MINIMUM NUMBER OF REGULATIONS

It is still unclear how many regulations should be defined and executed in our healthcare enterprise. The information office understands that no one can answer such a question, because the enterprise environment is changeable and the existence of the ideal and minimum number of regulations is negative in any current enterprise. All enterprises change their internal processes and environment to attempt to survive or defeat their competitors in their industry. Accordingly, the regulations should be appropriately adjusted before they adopt a new information technology inside their enterprises. On the other hand, if enterprises remove existing information technology from their workplaces, they should also refine their original regulations.

ONE GATE FOR ACCESSING ALL MATERIALS

Our healthcare enterprise completed the IBM restructuring project from 2004 to 2007 and created a single sign-on information portal with an in-house, customized program. It is thus predictable that some users would be worried about the strength of security protection. However, the outcomes of the question D3 (I prefer to use our new information system with the single sign-on functionality) in Figure 5 indirectly shows that most of the OIS users prefer such an implementation. That is, the sum of grade 4 and grade 5 of IOS is above 59.02%. On the other hand, the sum of grade 4 and grade 5 of IIS decreases a little and is not >50%. This may represent the fact that IIS users might still entertain some suspicions when using our self-developed information system.

Such a problem, that is, whether the information portal with a single authentication key solution is secure and appropriate, is widely

Fig. 5. Question D3 statistical graph for both outpatient and inpatient information systems in 2007.

Fig. 6. Question F4 statistical graph for both outpatient and inpatient information systems in 2007.

discussed by the researched enterprise's colleagues. If the portal login process uses only one interior key for identification, the process may lose its security strength and cause users to suspect that the inter-connected system protection is weaker than one or more keys. However, it is a trade-off and there is no optimal answer for the quantity of keys.

To strongly execute the single authentication policy, our superintendent required our information office to integrate the personal salary account query functionality inside the portal environment and attempted to change the computer utilization behaviors of careless and disobedient users in August 2007. Such guidelines were gladly received by our information office and some users will complain to the related execution department. However, most of the colleagues will gradually adapt to the policy, if they want to use the computer technologies that allow them to give correct responses without delay. In summary, the evidence indirectly shows that the clinical users accepted our administrative security policy.

THE NEXT STEPS

Imperceptibly, our healthcare enterprise will gradually adopt EHR and the information technology adoption will be highly involved. As such, we planned the related regulation modification schedule, which is based on the EHR production dates. For example, the mobile care unit solution will be on production at our inpatient nurse units in June 2008 and our IMC refined some regulations, such as NS.1 (network utilization management points), NS.3 (virtual private network management points), and SS.4 (health information system user privilege management regulation), to prepare for such process adoption and its related impacts.

Further, evidence from question F4 (I feel our new information system promotes our EHR adoption level) in *Figure 6* shows that ~40% of OIS and IIS users in our healthcare enterprise have strong confidence in achieving the EHR process. This evidence proves that the regulation's execution along with the new information system implementation is effective.

Conclusion

Our research proposed a generic preconsideration and postconsideration hybrid model, the AERA, for health information security management to reach the target of a mission-critical EHR process. The survey outcomes and evidential experiences from medical center users proved that our proposed architecture assists healthcare enterprises in satisfying the national e-Taiwan policy and in gaining ISMS accreditation, as well as encouraging the information office and enterprise administrators be prepared for the future electronically equipped hospital. Even though our original goal was to achieve smooth information security management within a tight security environment, the additional outcomes from our model were beyond prediction. We believe that the AERA's experiences can assist more enterprises to customize and refine their present bylaws directly, continuously, and recursively.

Acknowledgments

The authors acknowledge the contributions from all the IMC members and all the colleagues in NTU Hospital. Especially, thanks to Chief Tzu-Hsiang Yang, and Hsiu-Chen Chung, in the Information Systems Office, NTU Hospital from 2000 to 2009. The authors are also grateful to Ronald C. Merrell, M.D., F.A.C.S., and Charles R. Doarn,

M.B.A., Editors-in-Chief, *Telemedicine and e-Health*, and anonymous reviewers for their interesting suggestions, comments, and remarks.

Disclosure Statement

No competing financial interests exist.

REFERENCES

1. About us: statistics, National Taiwan University Hospital, Taipei, Taiwan. 2010. Available at www.ntuh.gov.tw/en/AboutUs/Statistics.aspx (last accessed February 10, 2010).
2. Sherwood J. SALSA: A method for developing the enterprise security architecture and strategy. *Comput Secur* **1996**;15:501–506.
3. Schekkerman J. *How to survive in the jungle of enterprise architecture frameworks: Creating or choosing an enterprise architecture framework*. Victoria, BC, Canada: Trafford Publishing, **2004**:13–90.
4. Farn KJ, Lin SK, Lo CC. A study on e-Taiwan information system security classification and implementation. *Comput Stand Interfaces* **2008**;30:1–7.
5. Coallier F. Standards, agility, and engineering. *Computer* **2007**;40:100–102.
6. Keblawi F, Sullivan D. The case for flexible NIST security standards. *Computer* **2007**;40:19–26.
7. Ross R. Managing enterprise security risk with NIST standards. *Computer* **2007**;40:88–91.
8. Ross-Lee B, Weiser MA. Healthcare regulation: Past, present, and future. *J Am Osteopath Assoc* **1994**;94:74–84.
9. Cheng PH, Lai F, Lai JS. A service-oriented healthcare message alerting architecture in an Asia medical center: A case study, *Int J Environ Res Public Health* **2009**;6:1870–1881.
10. Cheng PH, Hsieh SL, Chien TN, Chen YP, Su MJ, Weng YC, Chen SJ, Lai F, Lai JS. Understanding discrepancy: A conceptual persistent healthcare quality improvement process for software development management. In: Kordic V, ed. *Process management*. Austria, European Union: IN-TECH Education and Publishing, **2010**:327–338.
11. Organ TW. *Philosophy and the self: East and West*. Cranbury, NJ: Associate University Presses, **1987**:43–65.
12. Berger M. Bureaucracy East and West. *Adm Sci Q* **1957**;1:518–529.
13. Giles HA. The trimetric classic. 1910. Available at <http://users.openface.ca/~dstephens/trimetric.htm> (last accessed February 10, 2010).

Address correspondence to:

Po-Hsun Cheng, Ph.D.

Department of Software Engineering

National Kaohsiung Normal University

No. 62, Shenhong Road

Yanchao Township

Kaohsiung County

Kaohsiung 82444

Taiwan

E-mail: cph@nknknu.edu.tw; d90943006@ntu.edu.tw

Received: February 13, 2010

Revised: April 15, 2010

Accepted: April 22, 2010