THE TRUSTWORTHY COMMUNICATION ENVIRONMENT FOR SECURE ONLINE TRANSFER OF MEDICAL RECORDS

Boris Koyrakh
School of Information Science, Claremont Graduate University
boris.koyrakhb@cgu.edu

Acknowledgements

I would like to thank Professors Thomas Horan and Terry Ryan, and the Practicum-2003 Research Team Deborah Beranek Lafky, Brian Hilton, Haiqing Li, Bengisu Tulu, and Liyan Xu for their encouragement and support.

Abstract

This paper proposes a framework for electronic medical record (EMR) system implementation. Currently, the medical industry is experiencing a rapid increase in computerization. The medical companies are trying to improve and streamline business processes, which is leading to organizational changes. More and more physicians communicate with their patients by means of a desktop, notebook or pocket PC. On the way to a paperless medical office IS/MIS organizations need to create trustworthy communication environments, in which all communications are through computers, not pens and paper.

This research suggests a trustworthy framework of an EMR system, which provides a solution to the problems of secure on-line transmission of electronic signatures (e-signatures), attached to medical documents. The experimental model proposes a set of conceptual variables.

Keywords: *Business process, EMR system, framework, e-signature, secure online transfer of medical records*

Introduction

According to [2], the term electronic signature indicates various methods of signing an electronic message that (a) identifies and authenticates a particular person as the source of the electronic message, and (b) indicates such person's approval of the information contained in the electronic message. A digital signature is an example of an electronic signature. Currently, efforts to automate the medical industry face a problem with the secure online transmission of electronic signatures attached to documents. This problem is part of a larger set of challenges to secure online communications. These challenges include secure login and access to online information by medical practitioners, real-time communications, storage and update of information, and attachment of electronic signatures of responsible practitioners and online users. Although existing technical solutions for secure online transmissions are accepted by many companies who employ insurance adjusters [3], they are not accepted by medical companies associated with the U.S. Department of Veterans' Affairs (VA). The VA could benefit from having medical practitioners submit disability evaluation reports online.

The e-signature technical solutions are based on the existence of online certification authority (CA) companies and developers of security encryption algorithms (SA) who provide certain software packages to online clients [12]. In addition, stand-alone companies have a choice to either purchase security certificates or software components from CA or SA companies or to develop them by the company itself. Figure 1 shows a conceptual diagram of a secure connection between two companies involving online service providers.

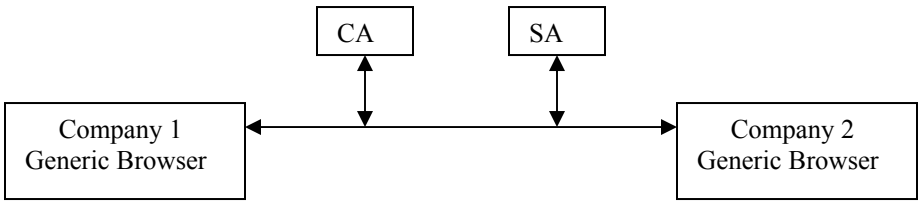


Figure 1. An Internet-based secure online transmission

The advantage of the approach shown in Figure 1 is that there exists only one efficient and fully automatic Internet connection, or online business process, between Company 1 and Company 2. However, the disadvantages are:

1) The security algorithm is subject to hackers braking it,

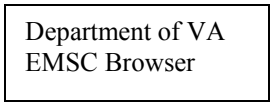
2) Users must follow specific security login procedures for retaining passwords and personal keys, and

3) The online connection must be protected from fraud, misuse, loss of messages and disconnections.

In cases where transmission security is critical, the disadvantages of the currently used solutions stated above are not acceptable. For example, the online transmission of a disability evaluation report with an e-signature is a sensitive issue. What is the effect of e-signature technology on the EMR system in the medical industry? This paper is devoted to the research topic of an EMR system with e-signature. It develops a trustworthy EMR framework for secure online transmissions, which lays out a foundation for further research and the improvement of business processes at medical service companies. The subjects of organizational change, business processes, and the EMR will be considered in application to a secure online transmission of e-signatures.

The practical problem of a secure online transmission of the e-signature at the EMSC company

The Electronic Medical Services Company's (EMSC) EMR system is described as a network server(s) containing databases of electronic medical records. Specifically, medical records of disability evaluation reports. Unlike paper-based patient records, communication systems and technological security tools are an integral part of the EMR system. The EMSC provides online checklists, worksheets and documentation to physicians. The business processes involve physicians, EMSC and the VA. Figure 2 is a diagram of business processes at the EMSC. Physicians use the online services in order to file reports to the VA. A physician fills out the online disability evaluation report and submits it to the EMSC. This saves doctors time and increases their availability for patients. According to [3], physicians also manually fax medical reports containing their signatures to the EMSC using manual faxing connection on the diagram. However, a manual faxing connection is not efficient for either EMSC or the physicians. After the report is verified, EMSC employees scan it into the computer and store it in the repository.



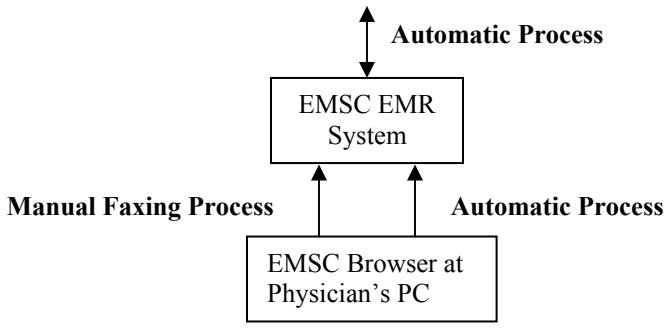


Figure 2. The diagram of current business processes at the EMSC

The EMSC simultaneously maintains two communications channels: One for fully automatic online services, the second for the manual processing of physician-signed reports following quality verification and signature authentication. The existence of the manual faxing process in Figure 2 can be explained by the e-signature problem, described in the introductory section of this paper. This leads to an inefficient manual business process at the EMSC.

Research for a general solution

Based on Figure 2, we can make several claims:

1. The EMSC's business model is to help physicians with online filing of disability evaluation reports to the VA.
2. The automatic EMR system, EMSC's primary business process, is challenged by the need of non-EMR manual business processes.

From this, it is clear that the EMR online business processes are critical for the EMSC. In fact, they constitute major organizational business processes. In support of our considerations we refer to the articles and books which describe the challenges and strategies of IS, EMR and e-signatures.

The e-signature problem is central to the EMSC because it impact the entire business. EMSC can improve its business processes only through solving this problem. On the other hand, the company might need to add many other EMR components. In order to find a solution to this research problem, we need to better understand the problem domain as diagrammed in Figure 2. We envision the ideal diagram with only one secure online transmission channel, which would solve the e-signature problem. The right way to start the research is to review literature on the relevant subject, and then explain why the problem still exists and how it can be solved.

The conceptual model of automating business processes

An existing technology partially solves the problem of e-signature, but is not fully accepted by businesses. Patel [17] states, "Historically, the level of sophistication of tools in a society reflects its intelligent activity. A tool is effective if it goes beyond what is already possible." We conclude that these tools help to solve important problems at this time, although the tools are not perfect, they relate to and reflect the level of development in society. Kernigan and Plauger [9] declare, that "a surprising number of programs have one input, one output, and perform a useful transformation on data as it passes through. Such programs are called filters….a careful selection of filters that work together can be a tool-kit for quite complicated processing." Gates [4] states, "current audacious goals include making the PC scale in performance beyond all existing systems, developing computers that "see, listen and learn…"" Figure 2 presents private browsers at the client's computers, which greatly improve the reliability and security of an online communication.

Ackoff [1] states, "It must be assumed that the system that is being designed will be deficient in many and significant ways. Therefore, it is necessary to identify the ways in which it may be deficient, to design procedures for detecting its deficiencies, and for correcting the system so as to remove or reduce them …three groups should collaborate: information systems specialists, operations researchers, and managers. The participation of managers in the design of a system that is to serve them, assures their ability to evaluate its performance by comparing its output with what was predicted". Ackoff assumes that

any system is not perfect. We need to identify, however, the deficiencies of the digital technology and all components of the automatic business process in order to design procedures to correct them and fulfill our criteria of effective performance. It follows that the involvement of managers, specialists and operations researchers is needed. According to Gates [4], a modification of the test system with a pre-set constant feedback loop becomes a process-control system. The process-control system "shows operators the cost of reduced efficiency. By attaching a dollar figure to operational parameters, the system is turning its operators into businesspeople, giving them information they need to run their units efficiently and a lot more responsibility to make decisions."

Ein-Dor and Segev [5] statistically evaluated organizational context variables contributing to the success of MIS. They draw a set of propositions based on controllable and partially controllable variables: organizational resources, organizational maturity, psychological climate, responsible executive, and steering committees. Propositions 20, 21 and 22 suggest that executive leadership, appointment of steering committees, and management support encourage a favorable psychological attitude toward MIS to promote success. A "human" aspect of the security issue is a stand-alone problem [6]. Building on these ideas, the users of e-signature technology will be expected to stick closely to the security procedures required by the EMR system with little room to diverge from them. The methods need to be developed to ensure that security passwords and doctors' private keys are protected. The EMR system, in its socio-technical aspect, needs to have special procedures to minimize fraud and misuse of the system. This aspect can be part of company security and management, which would also provide appropriate training and monitoring of involved users [6].

Marcus and Robey [7] discuss the causal structures found in theories about the relationship between information technology and organizational change. The process theory, emergent perspective, and mixed macro-micro level of analysis help to explain the effects of different factors on the acceptance of the e-signature technology by the medical services companies. Gates [4] notices "curiously enough, the managed care that many physicians love to hate may turn out to be the primary driver that extends information systems into patient care and returns control of patient care to doctors." The mutual interest of physicians, medical services and government can be a key for the organizational transformation of medical companies and for the resolution of the secure online transmission of e-signatures.

Based on this recent scholarship, we can draw the conclusion that the root of the e-signature problem now lies in social and organizational issues that contribute to the degree of acceptance of new technologies. The e-signature technology is here. As the overall quality of EMR system that uses e-signature increases at the EMSC, it will result in improved automatic business processes, and consequently performance. The diagram of trust relationships between partners is shown in Figure 3.

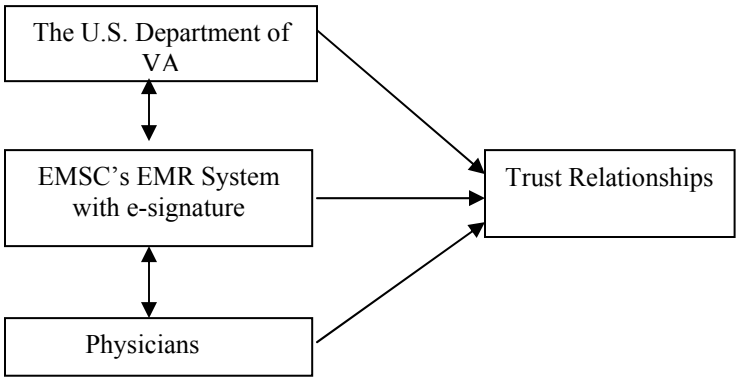


Figure 3. The web of trust relationships supporting e-signature technology

Trustworthy EMR Framework

In order to develop a high level of trust, which is necessary to achieve the performance level of EMR with e-signature, the diagrams in Figures 2 and 3 are combined into the Trustworthy Communication Environment in Figure 4.

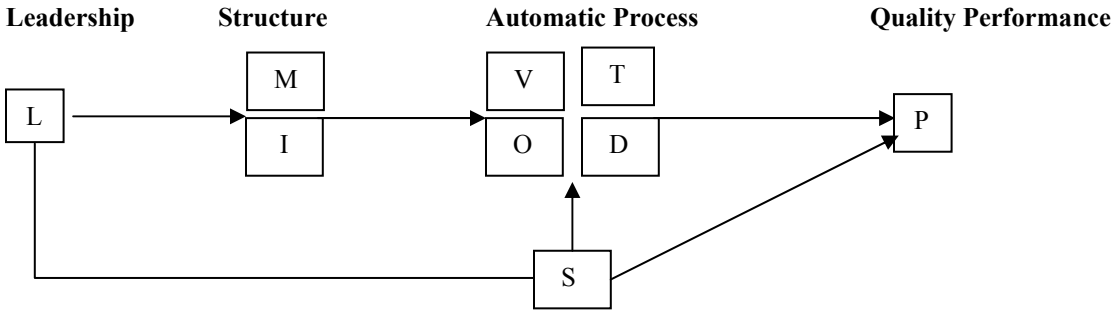


Figure 4. Trustworthy EMR Framework for automatic business process at the EMSC

In researching work on the Quality IT organization [13], Ravichandran and Arun Rai suggest a conceptual model of an IT quality-focused organizational system that aims to achieve a desired level of overall quality. They state, "A central theme of quality management is that technical and human aspects of a process must be managed in concert." The objective of the EMR is to support automatic business processes with the embedded e-signature in order to achieve a stable, within our parameters high Quality Performance of the overall system, and complete report of operational processes and the deficiencies of all components.

For this purpose, the EMR needs to have several conceptual constructs:

- (L) Top management leadership [13] symbolizing trustworthy computing environment. It can directly impact process characteristics and stakeholder participation.
- (T) E-signature technology and sensors to measure the quality of EMR automatic processes.
- (M) Management infrastructure sophistication component to implement monitoring and control.
- (I) IS staff at the EMSC.
- (D) Doctors to submit electronic medical reports with e-signature.
- (V) VA officials to receive electronic medical reports from the EMSC.
- (O) Operations researchers at the EMSC to design procedures for EMR system improvement.
- (S) Stakeholder participation, including employees, physicians and VA officials.
- (P) Quality Performance of the EMR system with output in the form of automatic online business process-control and embedded e-signature.

In order to evaluate an EMR trustworthy communication environment we intend to measure the reliability of the secure online transmission and its effect on the EMR system quality performance.

Experimental Model

In this experimental model, we detect several variables affecting the EMR system Quality Performance [16]:

- (R) Reliability of automatic transmission of medical reports with e-signatures. This variable is very important because it determines why one fully automatic business process is of higher quality for the clients than the two processes of automatic process and manual faxing process.
- (P) Performance. System performance depends on the use of the system, reliability and human factors.
- (O) Operations Research. O1 – problem finding activities, O2 – problem-solving activities.

- (A) Attitudes and perceptions. A1 - strictly and correctly adhering to the security procedures. A2 - preferences to use the secure online transmission. A3 – Information Systems (IS) support. However, there might be cases, when physicians would prefer to use "old" faxing method.

- (S) Situational factors. S1 - stimulating work environment, S2 - length of time in present position.

- (I) Personal factors. I1 - age, I2 – education.

- (D) Decision style. It affects the decision-making process and the use of the secure online transmission.

- (U) Use of fully automatic secure online transmission with e-signature. U1 – overall progress, U2 – planning, U3–working with clients, U4 – reporting.

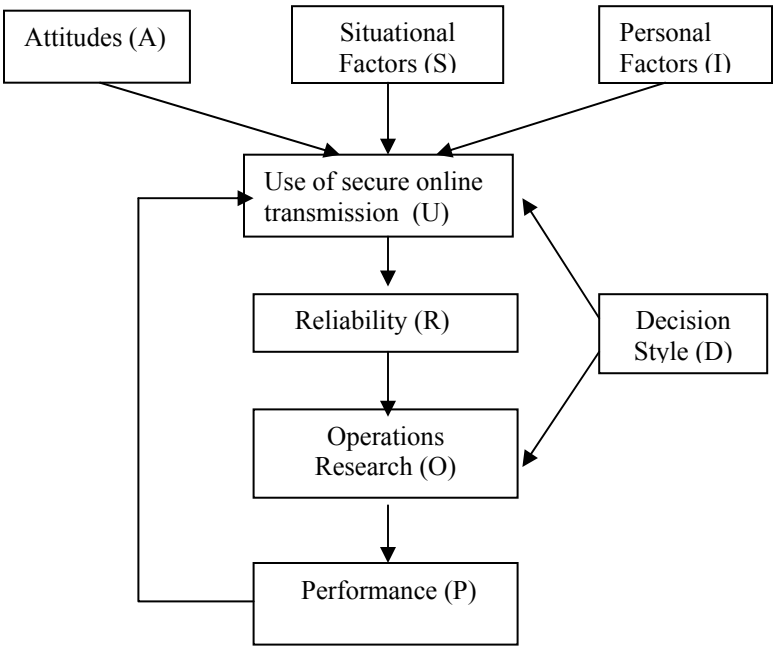


Figure 5. Experimental Model

Following Lucas [16], we also suggest two formulas for calculating Performance:

(1) $U = f(P, O, S, I, D, R, A)$

(2) $P = f(U, O, S, I, D, R, A)$

Formula (1) calculates U when operations researchers work on the tasks of problem finding (loss of messages, misuse, security issues, fraud, and alike). Formula (2) is for system improvement activities and for situations, when the EMR system operates within our parameters without problems.

Table 1. Variables in the study

Variable Class	Variables	Source
Performance (P)	P – profit, in dollars	MIS records
Reliability (R)	R – consistency or stability of operation	Calculated
Operations Research (O)	O1- problem finding, O2– system improvement	Questionnaire
Attitudes and perceptions (A)	A1 – secure login, A2 - computer potential, A3 – IS support	Questionnaire
Situational (S)	S1- work environment, S2 – time in present position	MIS records
Personal (I)	I1 – age, I2 – education	HR records
Decision Style (D)	D – affects the use of system and decisions	Questionnaire
Use of the secure online transmission (U)	U1 – overall progress, U2 – planning U3 – working with clients, U4 – reporting	Questionnaire

Table 1 contains a set of variables for determining the Quality Performance of the secure online transmission of medical records with e-signature at the EMSC. The goal of the study should be determining variables that contribute to Performance.

Conclusion

This research demonstrates the solution to the practical problem of the secure online transmission of e-signature. The trustworthy EMR framework at the EMSC was constructed, with easily identifiable constructs of Leadership, Structure, Automatic Process, and Quality Performance. The research suggests an experimental model for testing the trustworthy communication environment for secure online transfer of medical records.

References

[1] R. L. Ackoff, Management Misinformation Systems, Management Science, Vol. 14, No. 4, December 1967.

[2] Digital Signature Standard (DSS), U.S. Department of Commerce/NIST, Federal Information Processing Standards Publication, 2000 January 27.

[3] K. Noakes-Fry (15 July 2003), Challenges will limit Adobe and IBM's Digital Signature Effort, FT-20-5594. *Gartner FirstTake.* Retrieved January 29, 2004, from www3.gartner.com/resources/116200/116276/116276.pdf

[4] B. Gates with C. Hemingway, Business @ the Speed of Thought, Using a Digital Nervous System, Warner Books, 1999.

[5] P. Ein-Dor, E. Segev, Organizational Context and the Success of Management Information Systems, Management Science, Vol. 24, No 10, 1978.

[6] T. Huston, Security Issues for Implementation of E-Medical Records. Communications of the ACM, September 2001/Vol. 44, No. 9.

[7] M. L. Marcus and D. Robey, Information Technology and Organizational Change: Causal Structure in Theory and Research, Management Science, Vol. 34, No 5, May 1988.

[8] D. Severance and J Passino, Making I/T Work. An Executive's Guide to Implementing Information Technology Systems, Jossey-Bass, 2002.

[9] B. Kernigan and P. Plauger, Software Tools, Addison-Wesley, 1976.

[10] T. Zhou, Digital Signature Technology [Electronic version], Windows & .Net Magazine, February 1999.

[11] P. Palmer, Can PKI live up to its promise of meeting HIPAA requirements? [Electronic version]. Health Management Technology, April 2003; 24, 4.

[12] K. Noakes-Fry (01 May 2002), E-Signatures – Digital and Electronic: Perspective, DPRO-91585. Retrieved January 29, 2004, from http://ccrma-www.stanford.edu/~jhw/bioauth/andre/EsignPerspectiveMay02.pdf

[13] T. Ravichandran and Arun Rai, "Quality Management in Systems Development: An Organizational System Perspective", MIS Quarterly, Vol. 24, No. 3, September 2000.

[14] K. Pearlson, Managing and Using Information Systems: A Strategic Approach. John Wiley & Sons, Inc., 2001.

[15] P. Reynolds, A Primer in Theory Construction. Bobbs-Merrill Company, 1971.

[16] H. C. Lucas, Performance and the Use of an Information System, Management Science, Vol. 21, No. 8, April 1975.

[17] N. Patel, Emergent forms of IT governance to support global e-business models. JITTA: Journal of Information Technology, Theory and Application, Hong Kong, 2002.

[18] C. Robson, Real World Research, Second edition, Blackwell Publishers, 2002.

[19] R. Rogoski, Having it your way [Electronic version], Health Management Technology, May 2003; 24, 5.