Information Security and Privacy Policy Situation in Thai Public Healthcare Organizations

Chanin Luangingkasut,* Kamol Kaemarungsi,* Siwaruk Siwamogsatham,* and Asanee Kawtrakul*

Abstract

This research focuses on a study of information security issues in Thailand's public healthcare organizations. Lacking of security and privacy awareness by healthcare staffs may result in security violation of information systems. The objective of this work is to create guidelines for implementing security and privacy procedures to minimize security risk when utilizing Electronics Medical Records (EMRs) and deploying National Health Information System (NHIS) for ministry of public health in Thailand. In first stage, this study applies mixed methods research on medical staffs in order to determine their levels of awareness and attitude in protecting patients' privacy. The middle stage of this research involves determining security situation and collects related information on actual procedures when handling patient's data. In the final stage, this research recommends a set of measures to raise the awareness and to effectively secure the National Health Information System.

Keywords: Electronic Medical Records, Privacy Protection, Information Security

1. Introduction

To streamline the public healthcare system in Thailand, there is a need for information sharing of patient's medical records between different healthcare and non-healthcare organizations such as National Health Security Data and Social Security Data. Currently, there is a large amount of patient's information exchanged among these entities in which the information is critical and considered as secret between patients and doctor. The Ministry of Public Health of the Royal Thai Government does not have any standards on healthcare information. Moreover, many healthcare organizations have their own software which was developed independently by private software house companies. Consequently, there is no common data format that is easy for interchange and sharing. For instance, generating Thai citizen's health index based on scattering data from multiple sources will be very time consuming. Integration and sharing of information will be difficult to succeed if there is no national standard. Therefore, the National Health Information System (NHIS) committee has commenced the design and development of national standard for electronics medical data.

Because the medical records are relative in nature and often retrieved from different medical organization's information systems, in Thailand there are a number of important government information systems used by hospitals and local health centers such as systems from National Health Security Office (NHSO), Social Security Office (SSO), and Civil Servant Medical Benefit Scheme (CSMBS). Moreover, there are different requirements for data analysis such as health data for Thai civil service staffs [1], [2], health data for labors, and internal data from healthcare unit. From information security point of view, patients have every right to protect their medical records and their records must be disclosed only between patients and doctors. Information shared by several organizations is vulnerable to leaking and alteration by eavesdropping and malicious users [3], [4].

In order to increase confidence in information security on medical record database of National Health Information System, the NHIS committee needs a survey to determine the current status of security level in public organizations under the Royal Thai Government. The major objectives of this work are to study awareness level in information security of personals working under public healthcare organizations and to create security guidelines for the future development of Thai electronics medical record standards. The implication of this survey will help improve the information security policies for medical information system.

The organization of this paper is as follow. First, Section 2 review existing literature. Then Section 3 describes our research method in which we describe our subjects of study both personnel and their organizations. The research design of this study is also briefly summarized in this section. Then, in Section 4, we report the results of our research based on

* National Electronics and Computer Technology Center (NECTEC), THAILAND

interviewing technique. Then, in Section 5 we analyze the results and formulate a set of guidelines.

2. Literature review

This research is related to other researches in the area of privacy protection and security enhancement in information of public healthcare systems. We identified existing works which are relevant to our current work as follows. There are groups of researchers in [7] and [8] who proposed secured web-based solutions for protecting user's privacy and to increase security of healthcare information. In [8], the authors suggested a technique and developed an application to encrypt medical data and to authenticate the end-to-end nodes. However, Ashenden in [9] argued that the challenges in information security lied in the human factor where human skills and organizational culture have to be improved. The researchers in [9] suggested an approach to optimize organizational structure, processes, and relationships between management levels and end users. In this work, we followed the existing research works to create a set of guidelines for developing information security policy based on collaboration of all stakeholders in Thai's public healthcare systems. Note that the structure of the Thai's healthcare organizations is presented in [10]. The questionnaire used in this work is developed based on information security check list of the ISO/IEC 27001 and ISO/IEC 17799 [11].

3. Research methods and design

The objective of this study is to analyze security and privacy awareness on information systems used by public healthcare personals in Thailand. To measure the level of awareness, the authors initially had to understand existing medical information systems and processes used by those personals. We followed the guidelines of international standard in ISO/IEC 27001 [5] which is an information security management system (ISMS) standard. Note that we did not perform any auditing on public healthcare organizations according to all control points of ISO/IEC 27001. Using the lists of security control objectives and recommends from ISO/IEC 27002, the code of Practice for Information Security Management, we addressed the conformance in current security processes and policies with those recommendations in ISO/IEC standards. The output of this study will be in a form of recommendations to draft a policy and a standard for National Health Information System (NHIS). Figure 1 illustrates the research concept utilized by this study.

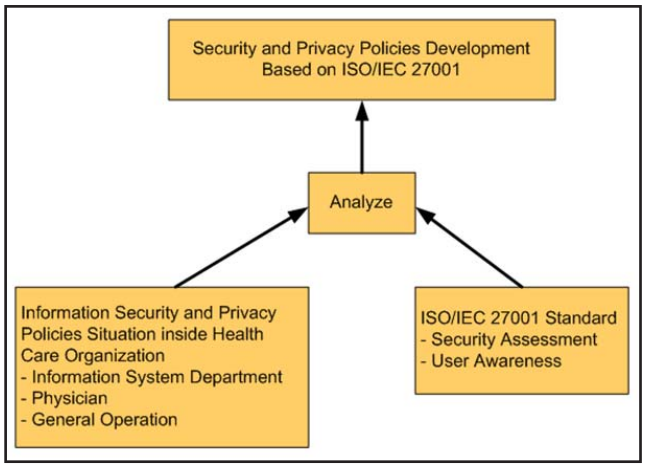


Figure 1 *Research concept*

This research took a mixed methods research approach [12] where we applied both qualitative and quantitative researches in single research to study our subjects. The mixed methods research is useful for studying a large number of sampling of people and organizations. It can generalize research findings when data are based on random samples of sufficient size [6]. The samples of subject were medical personnel who work in public healthcare units under the Office of the Permanent Secretary of Ministry of Public Health and medical schools in Thailand. We limited our study to those medical personnel involved in health information system or were users of electronics medical records. These personals were nurses, doctors/physician (MD), and IT administrators and staffs.

There are several data collection techniques for determining the awareness level to choose from such as interviews, questionnaires, and observation [13]. The main method of data collection in this study was interviewing approach. In this study, we selected in-person and small group interviewing approach to collect our data. The main reasons for this decision are to get the high response rate and highest volume of information. In-person interview is most likely to gain accurate information from subjects. We recognized that interviews may be time consuming and there might be extraneous information associated with the method. Moreover, a good interviewer requires a proper training. Since we visited the sites for interviewing and spent a lot of time to talk with sample subjects, we also used observation technique for additional data collection. Using observation, we could find out what people actually do during their operations. We recognized that our sample subjects may perform differently while they were being observed. We analyzed the results from our observation in

Section 4.2.

3.1 Public healthcare organizational structure

Organization structure of public healthcare in Thailand [10] can be divided into two major groups. The first group is responsible for policy and strategy of public healthcare. The second group of is actual healthcare offices that have medical staffs. Both groups are overseen by central administrators called the office of permanent secretary and the ministry of public health (MOPH), respectively. The policy and strategy group consists of three levels of national, provincial, and district offices as follows.

• At the national level, the bureau of policy and strategy is the central institute or central office of administrative strategy for healthcare. This office develops policy and plan for national healthcare. One of its goals is to improve healthcare personals efficiency through the use of modern technology such as information technology. However, the bureau later found out that there were too many separate information systems and required a lot of time for healthcare personals to fill data in each system. Thus, the bureau wants to minimize the procedures regarding to IT usages.

• At the provincial level, provincial public health offices are the offices of administrative strategy of health in each province. These offices focus on four tasks which are health policy and strategy, education, consumer protection, and health protection.

• At the district level, the public health office of district is entrusted with local administrative policy and strategy and every district offices within a province are under the provincial office.

The second group which is the actual healthcare units included in this study were categorized into medical centers, general hospitals, local hospitals, and primary healthcare centers. In Thailand, we classified type of these healthcare units by the number of beds in the building, and number of patients and medical staffs [10]. We characterize each of them in detail as follows:

• Medical center is the biggest hospital. It has the most complete equipments and has specialist physicians. This type of hospital is a center for nearby healthcare units in the area to refer the patient who is in coma. The capacity of medical center is usually more than 500 beds.

• General hospital is a provincial hospital located in major town of a province. This type of hospital has a potential to serve patients around its province. Some provinces may have the general hospital more than one location depending on its responsible areas. The capacity of general hospital is in between 200 and 500 beds.

• Local hospital is a mid-size hospital and has capacity between 10 to 200 beds depending on its responsible area. In general, a local hospital is located in a district.

• Primary healthcare center is the smallest unit that serves healthcare in sub-district area. It is very important healthcare unit that closely cares and protects health of people in its community.

3.2 Research design

Based on the methods and the identified subjects discussed above, we designed our data collection as follows. The number of personnel who were interviewed was 136 people consisted of staffs from information system department (IS), physician (MD), and general operation (OP) in healthcare organizations. These personnel are randomly selected for interviews. The total number of organizations that we collected data was 48 sites which included samples from both central and regional offices. We created a list of survey questions then visited the sites and conducted group interviews. The number of questions in each interview was 20 questions. The duration of data collection was between 1st July 2008 and 31st January 2009. Table 1 shows a list of factors included in this study.

Table 1 *Factors in research design.*

Factor		Quantity
Personal	IT staffs, physicians, general staffs	136 peoples
Organization	Central and regional offices, provincial and district offices, medical centers, general hospitals, local hospitals, primary healthcare center, non-government hospitals	48 organizations
Questionnaire		20 questions
Duration		7 months

4. Research results

In this section, there are two major results based on our mixed methods research. We report the quantitative results first and the qualitative results next in the following subsections. Table 2 summarizes the distribution of sample organizations which the authors visited and collected information by interviewing technique. In this research, we were interested in healthcare samples more than non-healthcare samples. Out of 48 samples, there are only 15 organizations that are in policy and strategy group while there are 33 organizations that are actual healthcare units. We expected that the actual

healthcare units were more vulnerable to violation of security and privacy of patients' information than the policy and strategy organizations, because they focused on nursing the patients and do not have dedicated IT staffs in their organizations. The electronic medical records are usually modified and utilized more frequent by physicians and general staffs of a hospital. Note that there were only 2 organizations which are non-governmental hospitals.

Table 2 *Number of sample organizations*

Factor		Quantity
Personal	IT staffs, physicians, general staffs	136 peoples
Organization	Central and regional offices, provincial and district offices, medical centers, general hospitals, local hospitals, primary healthcare center, non-government hospitals	48 organizations
Questionnaire		20 questions
Duration		7 months

Table 3 *Number of sample organizations*

Organization/ Department	Detail	Summary
Central Office/ Head Office	Information System = 15 Physician = 7 General Operation = 20	42
Provincial/District Public health Office	Information System = 2 Physician = 2 General Operation = 8	12
Medical Center/ General Hospital/ Local Hospital	Information System = 13 Physician = 3 General Operation = 15	31
Primary Healthcare Center	Information System = 25 Physician = 3 General Operation = 11	31
Non-government hospital	Information System = 6 Physician = 2 General Operation = 4	39
Total	**Information System = 61** **Physician = 17** **General Operation = 58**	**136**

Population of our interviewees are summarized in Table 3 where the number of personnel were divided into three categories of information system staffs, physicians, and general operation staffs for each group of organizations. Note that even though there were physicians who work in policy and strategy organizations, they are not practicing medical duties. The physicians were the smallest samples of 17 interviewees while the information system and general operation staffs were the largest samples of 61 and 58 interviewees, respectively. Figure 2 illustrates the samples of our interviewees. Note that the number of doctors or physicians is small compared to other staffs because the number of physicians is still not enough in Thai's healthcare system as any other countries.

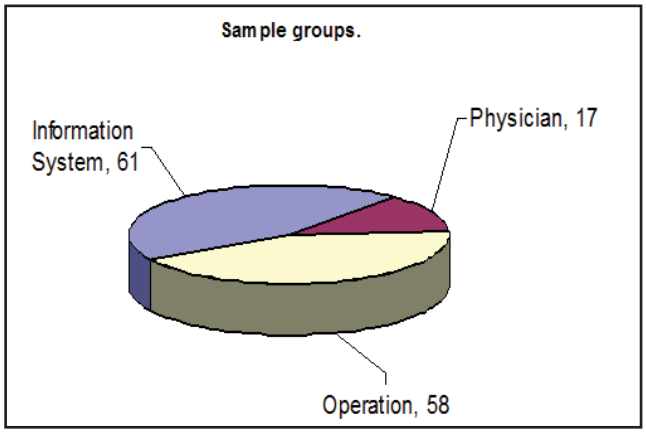
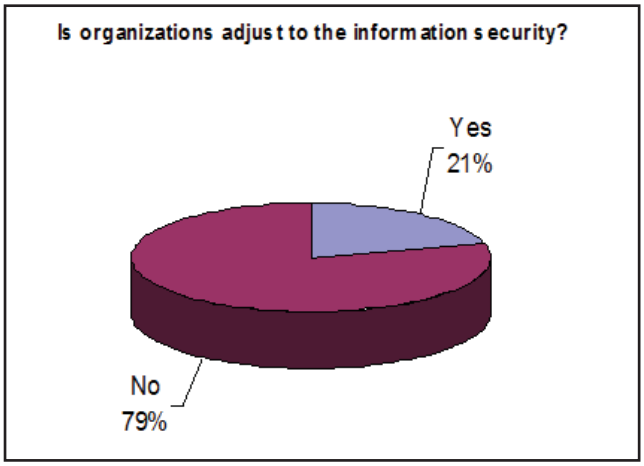


Figure 2 *Group of interviewees*

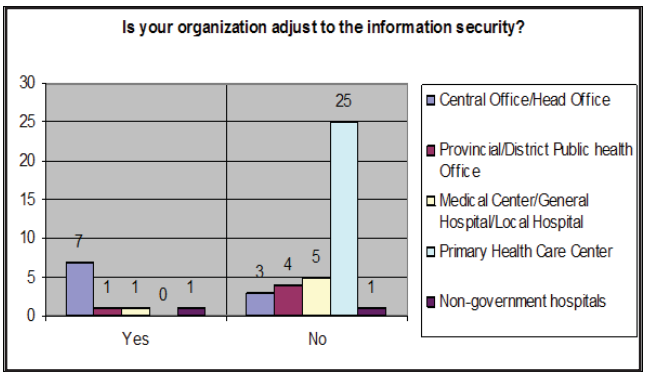
4.1 Quantitative results

Based on five out of 20 questions in our questionnaire, the authors have plotted the pie charts and bar graphs to visualize the quantitative research results. Each pie chart showed the overall response without any information regarding the type of organizations. On the other hand, we used the bar graphs to show different views on the same data and to show responses based on type of organizations. Note that the numbers in all of the results in this subsection are the counting of organizations. The questions in this group are related to information security and their awareness on information security policies and basic computer securities. The questions are listed as follows:

- Does your organization embrace the concept of information security?
- Does your organization have any information security policies?
- Does your organization have password policies?
- Does your organization monitor or keep log on computer and internet usages?
- Does your organization have any information security personal, technician, or supervisor?



(a)

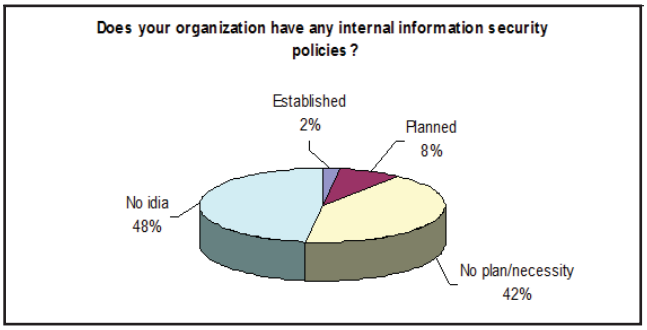


(b)

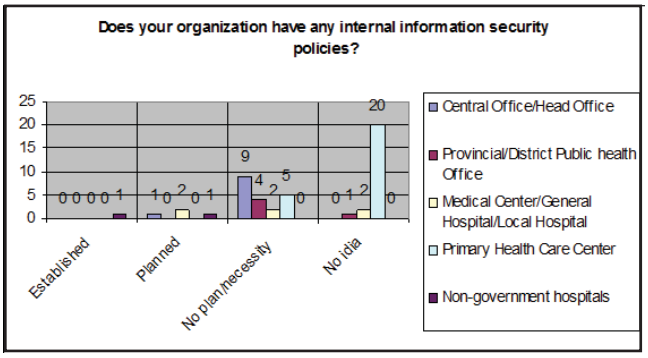
Figure 3 *Organizations that embraced the concept of information security.*

From Figure 3(a), the quantitative result of the first question clearly indicated that most of healthcare organizations were not aware of the important of information security. Almost 80 percents had no idea on how important the information security is to their organizations. When we separated the responses into the group of organizations that are aware and that are not aware, we found that most central offices/ head offices are well educated on the subject. On the other hand, most of the regional offices and in particular all primary healthcare centers (25 of them) did not recognize the important of information security. The result of this question suggested that regional offices should be improved.

In the second question, we determine how many organizations have internal information security policies. The responses are categorized into four groups of established policy, planned policy, no plan/necessity, and no idea. We found that 90 percent of sample organizations were either had no idea or did not see any necessity on information security policies as pointed out in Figure 4(a). Once again, all of the primary healthcare centers in the regional offices had no ideas on such policies. Only one organization had established security policies, which was a non-governmental hospital, and only four organizations had plans for creating some policies.



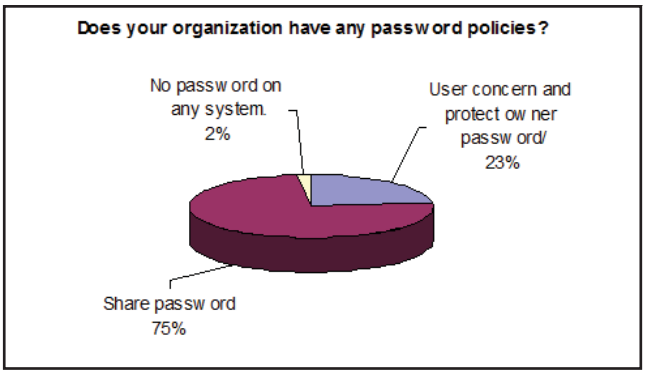
(a)



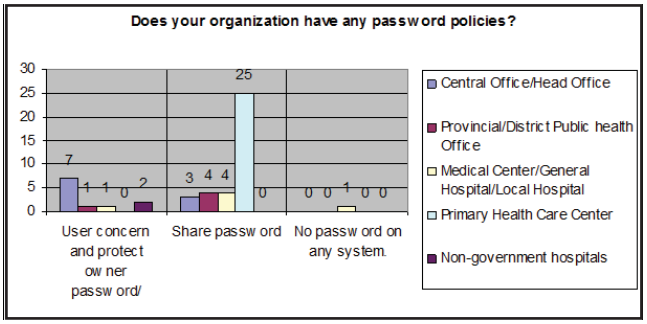
(b)

Figure 4 *Organizations that have security policies.*

The third and fourth questions are related to basic information security's best practice for any organizations. On the issue of computer's password policy, there are three groups of responses which are no password on any systems, sharing of password, and concerning and protecting of passwords. In Figure 5(a), we found that 23 percents of the organizations had users who concerned and protected their usernames and passwords. However, there were 75 percents of organizations which their staffs shared usernames and passwords. All of primary healthcare centers were in this group. One organization which is a medical center did not have passwords on any systems. This is a serious problem for information security. In the fourth question, we found that only 27 percents of the healthcare organizations monitored and kept log of computer and internet usages as depicted in Figure 6(a). Once again, all of primary healthcare centers did not have any monitoring or logging capabilities as showed in Figure 6(b). Note that the Royal Thai Government enacted a computer crime law in 2007 in which there is a requirement on keeping a log for computer traffics in most organizations for 90 days.

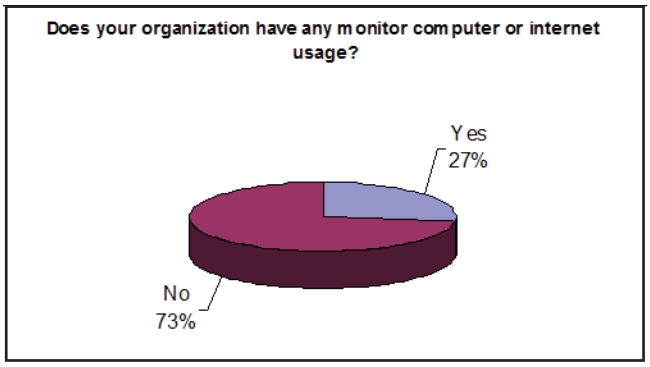


(a)

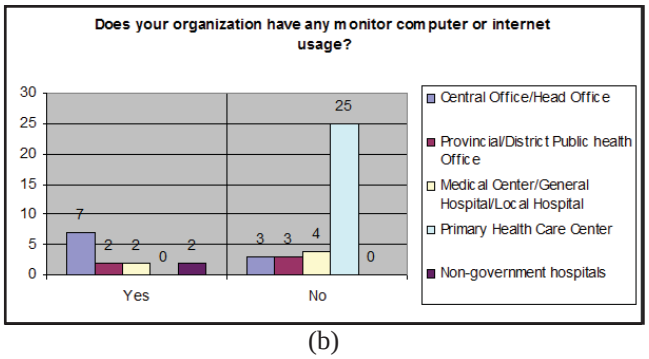


(b)

Figure 5 *Organizations that have password protection policies.*



(a)

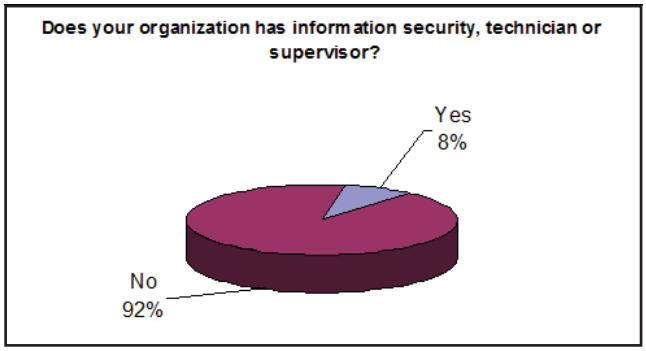


(b)

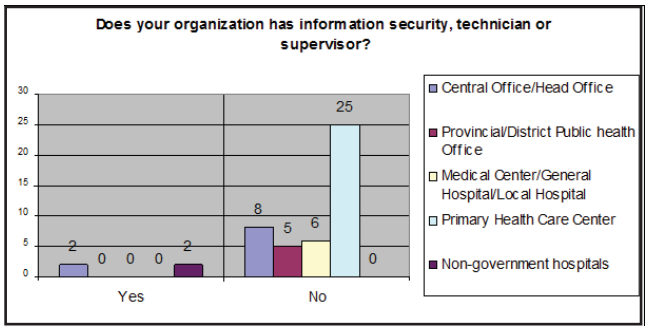
Figure 6 *Monitoring of computer or internet usage.*

Finally, in the fifth question, we investigated on the number of information security staffs, technicians or supervisors in those organizations. The result in Figure 7(a) is clear that only eight percents or four organizations had information security staffs. A staggering 92 percents of healthcare organizations did not have any information security staffs. All of primary healthcare centers have no information security staffs as showed in Figure 7(b).

The quantitative results based on five questions in this subsection indicated that most regional offices or hospitals in upcountry were not aware of information security. They were clearly lack of security policies and did not follow basic best practices such as secure passwords and logging of computer usages. Moreover, information security personnel were in short supply or not employed in these organizations.



(a)



(b)

Figure 7 *Organizations that have IT personals.*

4.2 Qualitative results

In this section, we analyze the qualitative results based on our interviewing questionnaire and observation on sites. Note that the results in this subsection are subjected to the authors experience in the industry of computer and information security. We conclude three major information security issues found in samples of Thai's healthcare organizations. This reflects overall qualitative results.

4.2.1 Issue in computer network and information system security. The authors' observation on each site yielded some insights on status, necessity, and usage of computer networks and information systems in healthcare organization.

Currently, there are both Internet and intranet communications. For Internet communication, most of the sampled organizations subscribed to asynchronous digital subscriber line (ADSL) service provided by local internet service provider (ISP) in order to exchange electronic medical records (EMRs) and other information between regional and central offices. Each organization employs its own intranet and the size of the local network is depended on number of staffs and office's size in that organization. Most of the sampled organizations have server computers for hosting database and maintaining medical service data. However, some servers in regional offices were not protected by firewall boxes to prevent unauthorized access. On the software side, we found that some of the operating systems were not patched or updated to the latest versions. There were some reluctant due to the fear of incompatibility between the new version of operating system and existing software applications. The healthcare staffs were afraid of interruption of the normal services due to an upgrade. We found that most of the computer systems had anti-virus and anti-spyware software. For windows based operating systems, there is built-in firewall software installed in most computers.

4.2.2 Issue in information technology security's policy. Most of sampled healthcare organizations did not officially promulgate any security policy. Because information technology staffs and computer specialists in these organizations were insufficient, the staffs responsible for information systems and computer networks were medical statisticians or other staffs who were interested in computers. These staffs were trained for specific software applications or only studied from user manuals provided by central offices. Lacking of specialists or computer personals, who can effectively manage and enforce IT security's policy, is the major problem in small-size hospitals and regional offices. We found that most of large-size hospitals and central offices were ready for imposing IT security policy. Some hospitals were parts of universities in which they were well supported by IT department of the universities. One of our sampled organizations was a hospital in a medical college which had a lot of funding. The hospital's computers and network systems were well managed by computer specialists.

4.2.3 Issue in user's awareness in information security. Most of the staffs in hospitals, and policy and strategy offices can be classified as IT end-users. Due to the lack of IT specialists and technicians in these organizations, these end-users were not aware of the important of the information security and the privacy protection. They were not trained or educated for protecting themselves and other people's information. For instance, we found that the major computer security problem was in the usage of storage media such as USB drives or CD-ROM drives. These media were not free from malware and were used without scanning for malware by anti-virus software. When these unclean media were put into unprotected computers used for filing electronic medical records or computers connected to organization's networks, important data could be stolen or corrupted and networks could be attacked by malware breakout.

Based on information gathered from interviews, staffs in every primary healthcare centers had to fill a lot of data such as health report and EMRs via web applications. Most of the applications require large amount of information. More than one organization shared these data, but the staffs had to fill in the same set of information multiple times. Because primary healthcare centers and local hospitals had small number of staffs, these small organizations lacked of budget to hire necessary computer personals. Typically, there were two to three staffs on duty for filing electronic health records. The computer resources and Internet connection at small organization are often inadequate. Some of the staffs confessed that they often send medical reports outside their office hours by using more powerful computers at their local Internet cafés which have high-speed Internet connections. Based on the authors' experience, those local internet cafés have a lot of weak security points such as very little or no virus protection and no control gateway. Sniffer programs might be installed on some of these machines; thus, patient's privacy might be broken by eavesdropping of EMRs.

5. Discussions and guidelines

In this section, we discuss the finding and suggest a set of guidelines for minimizing the risk on information system and processing of EMRs. We summarized situation inside healthcare organizations which affects information and privacy. We realized that this work would lead to create a more specific set of guidelines for NHIS.

5.1 Discussions

Technical understanding of information security and privacy is still lack in most of regional offices and organizations. For example, we found that general staffs did not understand the purpose of personal firewall. There were wide security gap between regional and central offices where there were insufficient computer specialists to support information

systems and enforce information security policy. One approach to reduce the gap is to raise awareness for all staffs though training and disseminating necessary manual to regional offices. The problem of sharing username and password can be eliminated by pointing out the security problem and privacy concern.

Since the 2007 law on computer crime was enacted, most of the sampled organizations were prepared to comply with traffic log monitoring and network time synchronization rules. However, there are some important procedures missing in most of these organizations. For instance, there is no correct procedure for disposal of unused computer equipments. Anyway, there are some good signs that the executive officers are aware and support necessary training program on information security for relevant public healthcare staffs.

5.2 Guidelines

Based on the findings from both on-site interviews and observation, we developed the following information security guidelines. Policy developed using these guidelines should be promulgated by the Ministry of Public Health in Thailand and implemented in all sizes of public healthcare organizations. These guidelines can be divided into two groups which are policy-based and technical-based recommendations.

5.2.1 Policy-based guidelines.

• Executive officers of the Ministry of Public Health and every healthcare organization must recognize important of information security and privacy protection of patients.

• Executive officers must appoint security officers or commission who are authorized to develop security policy and raise awareness to all staffs.

• The security officers or commission must be recruited from every department in an organization and these representatives can communicate back to their departments.

• The appointed security officers and commission must have administrative power and full support from executive officers.

• Development of information security policy must be promulgated and announced as a project with responsible champion or project owner.

• Executive officers must sign the announced information security policy and periodically monitor the progress of implementation.

• Executive officers must allocate a budget for effectively development of information security in organizations.

• Executive officers must publicize the policy and open opportunity for participation of all staffs and allow them to pose any questions and suggestions regarding the policy.

• Executive officers must setup helpdesk service, provide consultant, and train staffs when implement the policy.

• Create information security policy for properly dispose of unused computers and hard disks according to US Department of Defense clearing and sanitization standards.

5.2.2. Technical-based guidelines.

• Ensure that all computer systems have personal firewalls, antivirus, and antispyware.

• Ensure that all software and operating systems are patched to the latest update to minimize vulnerabilities.

• Do not allow un-authorized software to be installed on important computers related to EMRs.

• Each staffs must use their own passwords to logon to a system.

• Ensure that there are traffic monitoring software or systems installed to comply with Thailand's computer crime law.

• Ensure that all unused computer are disposed properly and ensure that all organizational, personal, and patient's data are deleted.

• Ensure that patient's data are transmitted through proper communication channels and free from eavesdropping.

6. Conclusions and future works

This work described our mixed method research on Thai public healthcare organizations. We reported on preliminary findings of information security and privacy protectionpolicy and situation. The results will be used to develop EMR standard in Thailand. We pointed out risks in current medical information system and medical staffs. A set of guidelines was suggested at the end of this manuscript which was reported to NHIS committee for further analyze and determine future plan on future information security for NHIS project. We hope that our initial guidelines will lay a ground work for reducing risks and vulnerabilities in Thai medical system. There are still a lot of works for developing a set of guidelines for creating a national standard for EMRs and secured procedures for information exchange.

7. References

[1] Bureau of Policy and Strategy Information Announcement; http://bps.ops.moph.go.th

[2] Healthcare Information System; http://healthcaredata.moph.go.th

[3] R. J. Anderson, "A security policy model for clinical information systems," *Proceedings of the* 1996 *IEEE Symposium on Security and Privacy*, pp. 30, 1996.

[4] R. J. Anderson, "Security in Clinical Information Systems," *Computer Laboratory*, University of Cambridge, pp. 1-34, 4th January 1996.

[5] W. Boehmer, "Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001," *The Second International Conference on Emerging Security Information, Systems and Technologies*, pp.224-231. 25-31 Aug. 2008.

[6] S.C. Petter and M.J. Gallivan, "Toward a framework for classifying and guiding mixed method research in information systems," *Proceedings of the 37th Hawaii International Conference on System Sciences*, Vol. 10 pp. 5-8 Jan. 2004.

[7] S. Sampath, R. Iyer, K.S. Sridharan, R. Mukkamala, and S. Kapoor," Secure Web-Based Sharing of Health Information Services Using Ad-Hoc Dynamic Coalitions," *Fifth International Conference on Information Technology: New Generations*, pp.297-302, 7-9 April 2008.

[8] B. Alhaqbani and C. Fidge, "Privacy-Preserving Electronic Health Record Linkage Using Pseudonym Identifiers", *10th IEEE International Conference on e-Health Networking, Applications and Service*, pp.108-117, 7-8 July. 2008.

[9] D. Ashenden, "Information Security management: A human challenge?", *Information Security Technical Report*, Vol. 13, No. 4, pp. 195-201, November. 2008.

[10] Bureau of Health Service System Development, "Guideline for Development Service System in Secondary and Tertiary Units," pp. 1-199, 2007.

[11] Thai Computer Emergency Response Team, *Information Security Check List based on ISO/IEC* 27001 *and ISO/IEC* 17799, pp. 1-153, 2007.

[12] R. B. Johnson and A. J. Onwuegbuzie, "Mixed Method Research: A Research Paradigm Whose Time Has Come," Educational Researcher, vol. 33, no. 7, pp. 14-26.

[13] Lee and Roadman," Linking Needs Assessment to Performance Based Evaluation," *Performance & Instruction*, 1991.