Information Security Sharing of Networked Medical Organizations: Case Study of Remote Diagnostic Imaging

Masayo Fujimoto, Koji Takeda, Tae Honma, Toshiaki Kawazoe, Noriko Aida, Hiroaki Hagiwara, Hideharu Sugimoto

Information Security Sharing of Networked Medical Organizations: Case Study of Remote Diagnostic Imaging

Masayo Fujimoto[1], Koji Takeda[1], Tae Honma[1],
Toshiaki Kawazoe[2], Noriko Aida[3], Hiroaki Hagiwara[4], Hideharu Sugimoto[5]

[1] Fuji Xerox Co., Ltd., [2] Fujifilm Medical Co., Ltd.,
[3] Kanagawa Children's Medical Center, [4] Yokohama City University Hospital,
[5]Jichi Medical University and Hospital,
Fuji Xerox Co., Ltd. Roppongi T-CUBE 15F,
Minato-ku, Tokyo 106-0032 Japan

Abstract. Increasing usage of ICT in medical organizations raises the issue of information security. This research study focuses on, and analyzes technology and management aspects for, information security of networked medical organizations through a teleradiology case study. A 'workshop' to gauge risk assessment was also established in which stakeholders, such as patients and radiologists, discussed the risk threat inherent in teleradiology. Based on this discussion, technological, organizational, physical, and personal security countermeasures were developed and organizational rules for networked organizations created. We conducted a step-by-step approach in which the second medical organization referred to the first medical organization's process and rules, and found that this approach was both efficient and effective. However, we also discovered that many internal and external adjustment works for each medical organization exist. To solve these issues we proposed two societal functions for audit and supportive institutions to handle such issues as compliance and education.

Keywords: Teleradiology, Remote Diagnostics Imaging, Information Security, Personal Information Protection, Risk Management, Cooperation of Medical Organizations

1 Introduction

According to the OECD health data 2009, the number of CT/MRI per million people is 96.1/42.7 in Japan. This number is quite large in comparison to other OECD member countries. However, this fact alone does not necessarily explain the higher quality of medical service provision. The reason for this is the shortage in number of Diagnostic Radiologists in Japan. We might be able to solve this issue by increasing the number of Diagnostic Radiologists. Although this approach is effective, current diagnostic imaging raises another issue. Because of enlargement and deepening of expertise in this field, together with the evolution of technology, it is difficult for every medical organization to employ specialists. Therefore, medical doctors,

organizations, and government have been challenging diagnostic imaging by using information and communication technologies (teleradiology). Some services have been introduced to market on a commercial basis, but we still have many medical doctors and organizations that hesitate to use teleradiology because of information security concerns, especially in protection of personal data. In order to further promote use of teleradiology, we need to develop effective information security procedures in order to reduce teleradiology accidents that arise from improper technology usage and management. It is important to encourage teleradiology usages that meet societal safety requirement. Based on the recognition of these problems, we performed an experimental study in which two medical institutions exchanged diagnostic images via an information network. In particular, we focused on the information security management aspect in this study.

2 Settings and Focuses of This Study

In the first section we introduce the three organizations that join this experimental study, in the second section we explain the information and communication technologies that are used in this project, in the third section we show the scope of this study, and the final section we describe the focus of this study.

2.1 Three Organizations

This case study involved the following three organizations, 1) Yokohama City University Hospital (YCUH), department of radiology, 2) Kanagawa Children's Medical Center, department of radiology (KCMC), and 3) information processing providers. Yokohama City University Hospital, department of radiology employs nine radiologists and has CT, MRI, PET/CT, and PACS facilities. Regarding information system management and other operations that relate to this study, the medical information and business administration departments also have responsibilities for whole organizational management. Kanagawa Children's Medical Center is a Kanagawa prefectural hospital and also has CT and MRI facilities. The department of radiology employs three radiologists, two of which are specialist in pediatrics diagnostic imaging. A person employed in the business administration department also joined this study. Information processing providers include three organizations. The first organization is a telecommunication company that provides network infrastructure, the second organization is a PACS provider, and the third organization provides mainly services and advice on internal network designs, system operations, and management.

2.2 Explanation of the Remote Diagnostic Imaging Systems and Operations

In general, diagnostic imaging for single organizations usually goes through the following steps,
(1) A radiological technologist stores medical images in a PACS system.

(2) A diagnostic radiologist diagnoses images and makes a report.
(3) A primary doctor decides on a treatment policy based on the images and the report form provided by the diagnostic radiologist.

In this study of the remote diagnostic imaging, we granted the assigned remote diagnostic radiologist permission to access to the PACS system to review permitted images for a defined period of time. Only the client diagnostic radiologist was able to grant access codes to the remote diagnostic radiologist and set the accessible period. The remote radiologist input the diagnostic report directly into the client diagnostic radiologist's PACS system. Diagnostic images were stored and displayed on the remote machine temporarily, but were deleted each time the remote diagnostic radiologist logged off the machine. The system account of the remote diagnostic radiologist expires after the defined period of time that the client diagnostic radiologist input initially.

2.3 Scope and Focus of This Study as an Information Security Management Case Model

The scope of this case model is described as follows,
(1) Two medical organizations that use the same network and computer systems.
(2) The intended information for this study specifically focuses on medical images and their related diagnostic reports.
(3) Each organization is managed independently.

The dot-line in the figure 1 outlines the scope of this study.

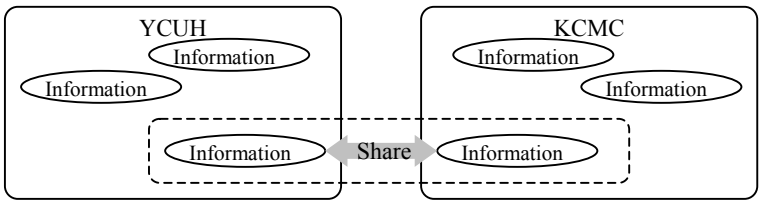

Fig. 1. Scope of this study

This study focuses on information security for remote diagnostic imaging. We can divide the information security into two types of countermeasures. The first is a technological countermeasure, while the second is a management countermeasure. Information security is constructed by combining these actions. In order to select the appropriate countermeasures we need to employ a risk management process. This study covers not only the technological countermeasures, but also management countermeasures. In the case of remote diagnostic imaging where more than one organization provides services, we face more complex management challenges than in the management of a single medical organization. Participants may agree on the same technological security countermeasures, but the management approaches differ depending upon each organization. Participants may need to agree to each other's different management systems. Therefore, in this study, we focused on security management and clarified the discussion points, aiming to discover an effective implementation method to solve the problems.

2.4 Past Studies and Relevant Legal Frameworks

Past Studies. In Japan, a number of studies that focused on organizational information security management have been conducted. For example, Hori discussed both technological security countermeasures as well as organizational countermeasures [1]. A number of books about information security have also been published. For instance, Doi et al. published a book to educate information security managers. The contents of the book also included sections on security management countermeasures [2]. In medical field applications, Tanaka studied personal data protection, and included organizational management countermeasures based on her findings drawn from meetings with medical organizations [3]. There was also study performed on information security incidents in medical institutions [4]. In the case of information security technology, many studies have been performed. In particular, a number of studies on network security have also been performed, as well as many other studies on the methodology of information security management and personal information protection. We also found documents that pointed out the importance of these studies and practices. Some similar studies in medical institutions were also performed. However, there are few studies conducted on management methods for sharing medical information and diagnostics with multiple medical institutions.

Relevant Legal Frameworks. The legislation relating to remote diagnostic imaging is complex and diversified in Japan. For example, we have the Medical Service Act, the Medical Practitioners Act, and the Personal Information Protection Law related guidelines. Because we want to focus on the practice of the remote diagnostic imaging and information securities in this paper, we would like to briefly outline the Personal Information Protection Law and discuss their relationship to management practices in this section. The Japanese Personal Information Protection Law went into effect in April 2005. The law is constructed in four parts. The first is the basic law that is applicable to both public and private sectors. The second is the general law and it is divided into the laws for both the public and private sectors. The third is the law established specifically for priority areas, such as medical, finance, and information and communication fields. The final law is a set of guidelines that each state minister in charge establishes accordingly. This legal framework makes the participating organizations' operations very complicated. For example, in this case study, the YCUH is owned by the city of Yokohama, while Kanagawa Prefecture owns the KCMC. Thus, different regulations of local governments are applied to each. This type of complexity may happen in international situations arising from difference among legislations and societal institutions in each country. We examined the method that medical institutions can enforce to secure remote diagnostic imaging under such a complicated environment.

3 Case Study

In this chapter, we explain the development procedure for the information security management system that we conducted in this study. In section 3.1, we will outline

the work flows and explained the four phases(section 3.2 to the section 3.5).

3.1 Process Carried Out in This Study

In this study, we mainly focus on risk management of information security for remote diagnostic imaging. Risk management here means the process of risk assessment and risk treatment. Risk treatment includes technological, organizational, physical, and personnel countermeasures. We practiced these risk management process and PDCA cycle. In the early days of this study, we discussed security with medical institutions connected in a network as a single group. We were going to build one management rule for all related organizations. However, we changed this approach because of their differing sizes and management methodology and decided to follow the measures described in table 1 and figure 2.

Table 1. Procedures in this study

Actions	Description	
1	Risk assessment by workshop	1st-phase
2	Information system design (include technological countermeasures)	
3	Information security management system design for YCUH	2nd-phase
4	Information security management system design for KCMC	3rd-phase
5	Agreement of two organizations	4th-phase

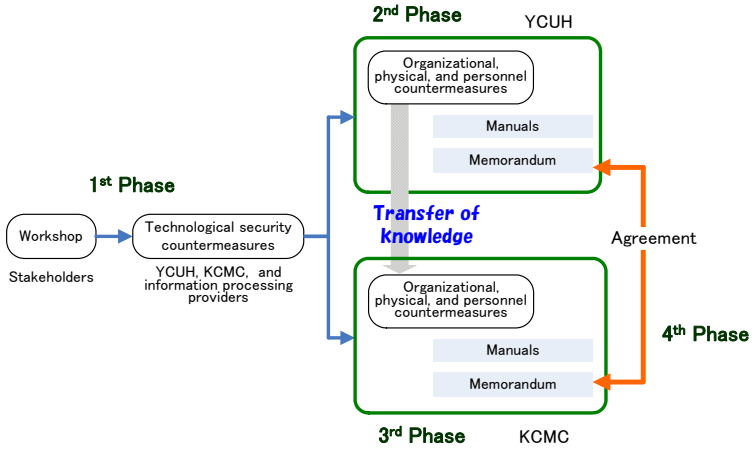

Fig. 2. Overview of four-phase process

3.2 Risk Assessment and Security Technology Selections (1st Phase)

In the September of 2006, the YCUH and the KCMC began discussions on the availability of remote diagnostic imaging. In February of 2007, diagnostic radiologists and information system engineers formed a project team. Through these discussions members shared their perceptions that information security is one of the most important requirements for the project.

Workshop. In June of 2007, the project members held a workshop and invited stakeholders to discussed risk factors. These stakeholders include the following people.

Diagnostic Radiologists, Patients, Hospital Directors, Practitioners, Clinicians, Radiological Technologist, Doctors from medical Information Science Department, Members of Administrative Department, Government Representatives, and System Vendors.

Thirteen stakeholders and one facilitator joined the workshop during two days, and pointed out 152 threats. Redundancies were extracted and the remainder aggregated into 76 threats that we decided to set countermeasures for [5].

Technological Countermeasures. Based on these threats we decided on technological countermeasures. In this experiment, the project members in the medical organizations and system vendors discussed these countermeasures. As examples of these technological countermeasures, we would like to explain the following two technologies that we selected.

(1) Technologies to deal with wiretapping threats to networks
(2) Technologies to deal with spoofing threats from fake remote radiologists

Firstly, for technologies to deal with wiretapping threats to networks, we employed VPN and SSL. We also compared IP-Sec, but selected VPN because in consideration of maintenance costs and compatibility to the spoofing threat countermeasures we employed. We assumed it would be a suitable countermeasure to spoofing attacks, and it had the lowest maintenance costs and higher compatibility than IP-Sec. Secondly, for technologies to deal with spoofing threats, we selected a client certification function of SSL. In normal client certification, a secret key is stored on a PC, but with this method, if malicious persons can successfully access the PC, they can pretend to be the legal owner of that key. In order to solve this problem, we stored the secret key to a biometric device. As a result, we were able to build a structure that gives permission to access the PACS server only to the person who succeeded in passing all device possession certification, biometrics authentication, and client certification of SSL. This certification scheme required some additional operations such as the publication management of the certificates and distribution management of the certification devices. However, system vendors could operate the systems as a part of their PACS maintenances functions. We carefully chose low-cost, widely available technologies, and by combining these technologies, achieved a higher level of security.

3.3 Risk Management in Yokohama City University Hospital (2nd Phase)

Having decided upon the technological countermeasures, we discussed organizational, physical, and personnel countermeasures with Yokohama City University Hospital (YCUH). In order to make these security countermeasures practical, we finalized the organization system and devised official regulations (figure 3).

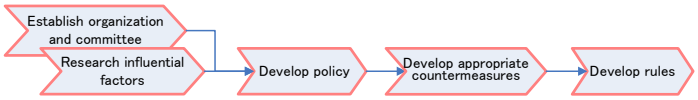

Fig. 3. Information Security Management Process in the Yokohama City University Hospital (YCUH)

Establish the Organization and the Committee. We developed the organization system and established an internal committee for decision-making. The organization system and the committee were both located in the department of radiology, and we invited members from both the medical information department that manages the information and communication system of the hospital and the business administration department that manages personal information protection for the hospital to attend. In the case of the YCUH, we successfully obtained the cooperation of other sections, and assumed that the workload for adjusting the different rules and manuals required would take considerable time to complete.

Research the Influential Factors. We investigated influential factors both outside and inside the YCUH in the following three categories. Firstly, we researched the legal requirements. We found out that the guidelines published by the Ministry of Hearth, Labor and Welfare related deeply to our project. One guideline focused on information security of medical information systems [6]. The other guideline covers personal data protection for medical and care organizations [7]. In addition to these, the city of Yokohama also published guidelines for city-owned public organizations that the YCUH must also comply with [8]. Secondly, we researched internal existing rules and manuals. We found that the personal data protection manual and information security policy had already been defined. In particular, the information security policy included system security countermeasures. We had to confirm that consistency existed between our technological countermeasures for remote diagnostic imaging and the hospital's information security policy (figure 4). Thirdly, we researched current operations for diagnostic imaging through interviews with diagnostic radiologists, including the physical environment and the movement of patients in the Radiology Department.

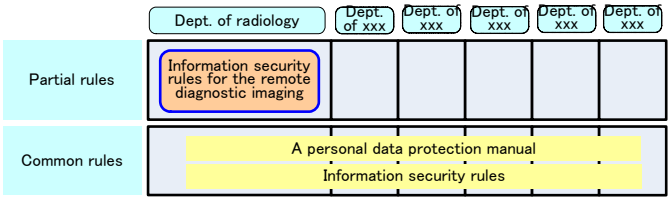

Fig. 4. Organize the relationship of hospital rules

Develop the Policy, Appropriate Countermeasures, and Rules. Firstly, we formulated a basic security policy for this remote diagnostic imaging, and then discussed and adopted appropriate countermeasures. Secondly, we implemented countermeasures and prepared manuals for organizational operations. Through this process we found that it was difficult to work on developing a risk management

system based on both risk assessment and legal requirements at the same time. Therefore, we developed our information security management system first, and then we checked its adaptability to both the legal demands and the required guidelines. Through this process we were able to appropriately develop the manual to suit the process.

3.4 Risk Management in Kanagawa Children Medical Center (3rd Phase)

The KCMC adopted same technological countermeasures by collaborating with the YCUH. Therefore, we needed to define organizational, physical, and personnel countermeasures. Two members from the KCMC participated in the discussion. One participant was a diagnostic radiologist and the other was a radiological technologist. At a comparatively early stage, we decided to develop two types of manuals, one for personal data protection and the other for information system security. The reason for this was that the radiological technologist has been taking care of information system security and then we thought that it was effective to maintain consistency between both the person in charge and the charge domain. In comparison to the YCUH, the KCMC was quite small in terms of the number of people who could work for remote diagnostic imaging. Therefore, we employed a different organization system. For example, we reduced the hierarchy for management and, as a result, we could also simplify the approval processes.
Like the YCUH, the KCMC had a higher-level of official rules for handling personal data protection. We drew up a correlation diagram of relating rules (figure5).

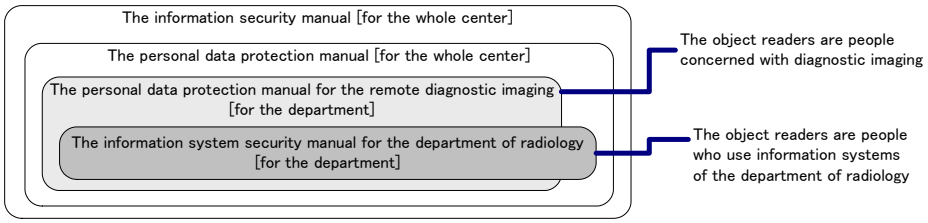

Fig. 5. Correlation diagram of rules

In this diagram, “the personal data protection manual for the remote diagnostic imaging” had been newly developed. “The information system operation manual for the department of radiology” had been revised to respond to operational changes by adding these remote diagnostic imaging activities. Discussion meetings had been held several times. For example, we discussed whether or not to develop a new system operation manual specifically for the remote diagnostic imaging, but we decided to revise the existing system operation manual for the system in the Radiology Department. Because the same radiological technologist mainly took care of both operations, there was no reason to make two manuals. The participating radiologist and radiological technologist carefully checked the usability of the manuals. When creating these manuals, we paid specific attention to developing the contents in accordance with everyday activities.

3.5 The Exchange of the Memorandum (4th Phase)

Through the discussions, we gradually clarified requirements for each organization. Following this, members from both organizations discussed together and drafted a memorandum that included the following contents.

Organization Systems, Personal Data Protection, Access Control
Facility Management, Education, and Audit

4 Discussions and Suggestions

In this section, we explain the results of this experiment, and also discuss problems in the practices that became clear as a result of the experiment. In the case of the problems, we would like to give some suggestions on how to solve them.

4.1 The Effect of the Approach Observed in This Experiment

In this experiment, we tried to find a useful methodology to establish a total security management system to use when we connect organizations together via networks and share information. Rather than first lay down a set of common security management countermeasures, we adopted a sequential method. The result showed that this method is useful at least for connecting two organizations.

In this case study, the two organizations are quite different in terms of organizational sizes and management cultures. For example, six people from three different sections attended the discussion meetings to make the manuals in the YCUH, while only two people from the Radiology Department joined the meeting in the KCMC. This reveals that in comparison to the KCMC, the YCUH have to select countermeasures under complex coordination among different internal sections. Thus, even if the radiologists of the two organizations gather together to try to select common countermeasures, the process does not run smoothly. This process may take a lot of time and involve considerable readjustment works. Even though they use the same technologies and accompanying technological countermeasures, the best way to establish security management differs greatly depending upon each organization.

The approach that we tried in this experiment facilitates construction of the appropriate system of administration that matched the individual organization, and that can set common rules.

In addition, for the wider development of rules and manuals, the individual organization can develop these without the know-how and experience of the rule for manual making by taking the rules and manuals of another organization into account. This approach also makes it possible to develop rules and manuals that reflected the circumstances of each organization. For instance, in this experiment, the number of discussions that we needed to hold with the KCMC was less than half the number required with the YCUH. It may be said that our method was effective even if we take into consideration that the organizational size of the KCMC is smaller than that of the YCUH. It is thought that this approach reduces the workload because we were able to use the rules and manuals that we developed for the YCUH as reference materials in

developing these items for the KCMC. If we continually apply this method to many different organizations, we may be able to establish a universal set of fundamental rules that may help other organizations reduce their workloads.

4.2 The Problems That Became Clear Through the Experiment

Adjustment Load for Each Organization. In generally, many medical institutions already have comprehensive rules to covering personal information protection and technological security countermeasure for information and communication systems. In this case study, the YCUH already had a comprehensive set of rules and manuals covering personal data protection for both the university and the hospital. The KCMC also has rules and manuals for personal data protection for its medical center. These organizations may not have factored in the situation when connecting to outside networks or for sharing information when they developed their respective rules and manuals. Therefore, we had to review the mutual influences with these existing rules and manuals when we developed the new rules and manuals for our remote diagnostic imaging operations. This study clarified the problems encountered, the adjustment work required, and the burden concentrated on the sections concerned when we introduced a new management plan in a specific section, as in this case, on the Department of Radiology. In order to solve this problem, it might be useful to introduce a governance scheme in which the central administrative section transfers authority of restrictive rule development to each section. It is desirable to have a section governance structure in which a rule can be set when the person in charge connects to the outside organizations via a network to conduct information sharing. In this structure, the comprehensive rules function as a baseline security countermeasure and the section's original, and in most cases, the rules may have a higher level of security than the comprehensive rules. Without such a structure, the person in charge of each section must put in considerable effort to seek out the best way to adjust the rules, placing considerable burden of the person in charge. Although we might be able to set the rule to a comparatively high level for the whole medical institution that assumes outside network connection, this approach may increase the workload of all sections and this may not be productive. Thus, we recommend introducing structured information security governance.

Adjustment Load with Outside Constraints and the Connected Organizations. We also experienced difficulty to cope with outside environmental changes such as laws and regulations. Over the course of the project, we had to check compliance to several guidelines that were sometimes quite similar, but not quite same, or that overlapped. These laws and regulations have been revised and we have to monitor these changes and react in a timely manner. This is accompanied with a review and the change to rules and manuals, and we must take also the approval procedure inside the organizations and of the organization interval. When we also think about preparedness to potential lawsuits, we need to record every management decision-making processes and file all relating documents. In theory, these works possibly become a continual workload of the Radiology Department rather than on the whole hospital's administration. We must discus how to solve this problem of increased

workload and economic burden for practical use. In this study, we discussed the case of two organizations connected via a network and sharing information. Thus, we could use the method to exchange a documented memorandum. However, when we think about a situation in which more and more organizations join and share information in the future, this method may turn out to be a very complicated process. This may delay the spread of remote diagnostic imaging. Thus, we need to develop another approach to help formulate a formation agreement. It may be useful to establish international standards and guidelines to solve this problem, and work on this has already started. We also think that the establishment of some supportive social institutions would be useful for promoting teleradiology, including remote diagnostic imaging by networked medical organization communities (figure 6). As we discussed before, we must secure human resources or financing to deal with increased workloads. Especially, with the first process of building the security management system and auditing systems which needs much knowledge and work. Therefore, we would like to suggest developing the social institutions for supporting mainly the creation of processes and auditing. It is important to establish whether connected organizations can perform appropriate administrative tasks for security. As the number of organizations connected increases, audit work also increases. Therefore, it would be useful if the auditors of the third party inspect the security management of the individual organizations. This approach is both effective and efficient. In addition, in the medical field, hospital usability tests are performed widely. If we place security as one element of the hospital function, giving certification and rating under this framework will also be effective [9].

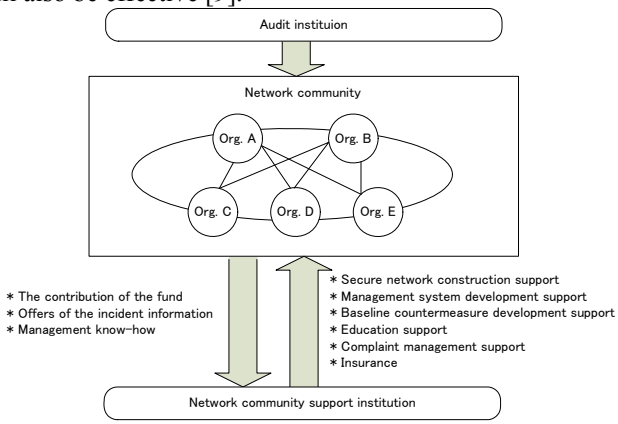

Fig. 6. Network community support institution

The network community support institution in the figure 6 is owned by the networked organizations. The institution may support a new member to develop manuals. It also can develop education tools, gather such information as legal change, standardization, and incidents from the other organization. However, these other organizations should carry out the audit.

5 Conclusion

In the medical field, a community is forming to deal with every specialized field beyond national borders. In the future, the need to share information in specialized fields is expected to increase. If we think about operations being connected in a network across borders, it is easy to assume that the issues that we discovered in our experiment will become more complicated. Especially, the differences in environmental elements, such as legal factors and healthcare policies, may influence the development of information sharing among networked medical organizations.[1]. For continual operation of information sharing, practical security management is indispensable. The implication of this study shows that the approach we tried in our project make it possible that each participating organization develops its own management system and at the same time maintains the security level for whole networked organizations. In order to promote further use of remote diagnostic imaging and other medical information sharing among medical organizations, it is useful to develop the method and social systems that can reduce the workload of medical organizations to acceptable levels and secure the security that society demands. We can expect to see further research in this field in the near future.

References

1. Hori, Y.: How to Build Common Understanding in the Implementation of Information Security Measures. Security Management, Vol.20, No.2, pp.19--27 (2006)
2. Doi, N. (eds.): Information Processing Information-technology Promotion Agency : Information Security instructional book - －Guide of Information Security Practice of Organization, Jikkyo Shuppan Co., Ltd (2008) (*translated by authors from Japanese)
3. Tanaka, M. : The significance of the Personal Information Protection Law in the Field of Japanese Medical Care. Master's Thesis of Institute of Information Security, pp.88-90/96-98, (2006)
4. Hiroshima, A. : Comments on the Personal Information Protection for Healthcare Providers. Security Management, Vol.19, No.2, (2006)
5. Hagihara, H., Fujimoto, M., Takeda, K., Honma, T.: Balancing of Effect and Risk of Medical Cooperation between Institutions using Information and Communication Technology. Japan Society of Security Management, 22nd National Convention Summary, pp.129-134 (2008)
6. Ministry of Hearth, Labor and Welfare. : Guideline for Safety Management of Medical Information System 3rd edition, pp.12-14, (2008)
7. Ministry of Hearth, Labor and Welfare. : Guideline for Appropriate Use of Personal Information in Medical and Care Institutions. (2006)
8. City of Yokohama, Code of Personal Information Protection of the City of Yokohama, http://www.city.yokohama.jp/me/shimin/joho/kokai/jorei/ko1.html, 2008-11-28
9. Hagihara, H., Aida, N., Sugimoto, E., Kawazoe, T., Matsuyama, K. : Establishment of Medical Cooperation System using Mutual Browsing Function of PACS. The 28th Joint Conference on Medical Informatics, pp178, (2008)

[1] The difference of the doctor license is a big issue. However, we have excluded it from our argument in this paper.