Original Article

Healthc Inform Res. 2011 September;17(3):162-171.
http://dx.doi.org/10.4258/hir.2011.17.3.162
pISSN 2093-3681 • eISSN 2093-369X

HIR
Healthcare Informatics Research

A SWOT Analysis of the Various Backup Scenarios Used in Electronic Medical Record Systems

Hwa Jeong Seo, PhD[1], Hye Hyeon Kim, MS[2], Ju Han Kim, MD, PhD[2]

[1]Medical Informatics, Graduate School of Public Health and Social Welfare, Gachon University of Medicine and Science, Inchon; [2]Seoul National University Biomedical Informatics, Interdisciplinary Program of Medical Informatics and Systems Biomedical Informatics Research Center, Division of Biomedical Informatics, Seoul National University College of Medicine, Seoul, Korea

Objectives: Electronic medical records (EMRs) are increasingly being used by health care services. Currently, if an EMR shutdown occurs, even for a moment, patient safety and care can be seriously impacted. Our goal was to determine the methodology needed to develop an effective and reliable EMR backup system. **Methods:** Our "independent backup system by medical organizations" paradigm implies that individual medical organizations develop their own EMR backup systems within their organizations. A "personal independent backup system" is defined as an individual privately managing his/her own medical records, whereas in a "central backup system by the government" the government controls all the data. A "central backup system by private enterprises" implies that individual companies retain control over their own data. A "cooperative backup system among medical organizations" refers to a networked system established through mutual agreement. The "backup system based on mutual trust between an individual and an organization" means that the medical information backup system at the organizational level is established through mutual trust. **Results:** Through the use of SWOT analysis it can be shown that cooperative backup among medical organizations is possible to be established through a network composed of various medical agencies and that it can be managed systematically. An owner of medical information only grants data access to the specific person who gave the authorization for backup based on the mutual trust between an individual and an organization. **Conclusions:** By employing SWOT analysis, we concluded that a linkage among medical organizations or between an individual and an organization can provide an efficient backup system.

Keywords: Information Storage and Retrieval, Electronic Medical Records, Medical Care Costs, Computer Security

Submitted: September 16, 2011
Revised: September 17, 2011
Accepted: September 20, 2011

Corresponding Author
Ju Han Kim, MD, PhD
Seoul National University Biomedical Informatics, Interdisciplinary Program of Medical Informatics and Systems Biomedical Informatics Research Center, Division of Biomedical Informatics, Seoul National University College of Medicine, 28 Yongon-dong Chongno-gu, Seoul 110-799, Korea. Tel: +82-2-740-8320, Fax: +82-2-747-8928, E-mail: juhan@snu.ac.kr

I. Introduction

As the paradigm of medical care services changes with the increased difficulty of management and lack of storage space for medical records, medical agencies and others have turned to the development of medical informatics for improving patient care, medical examinations and treatment. In recent years, health information technology (HIT) has become a major topic in medical information research [1,2]. Rapid changes in the medical environment have meant that medical records are increasingly kept with electronic form in computerized systems for keeping patient records offer many advantages.

As one of the health information technology, electronic medical record (EMR) systems are intended to keep track of a patient's entire health and medical history in a computerized, electronic format. By keeping these potentially vast records in this manner, they are more easily retrievable, and can make a patient's navigation through the healthcare system much safer and more efficient [3]. It has been started with the US federal government announcement since 2004, which was that a framework to accelerate the adoption of HIT, with the goal of creating an environment where EMR-related technological development could occur by promoting the reform of medical care services through technical innovation in medical informatics for most Americans within the next decade [4]. Physicians and practices would be using EMR systems with interoperable standards, allowing them to share laboratory results, such as computerized orders and prescription information, with hospitals and other health care facilities.

In Korea, the 'electronic chart' was introduced in 1990's, and the first complete EMR system achieving a 'paperless' and 'no-film' system, was introduced in 2003 at the Seoul National University Bundang Hospital. With the introduction of EMR systems, the quality of medical service has tremendously improved in terms of providing satisfactory systematic clinical information and reducing the times for medical examination and treatment [5].

EMR information must be securely backed up to prevent medical information from being lost or damaged in case of an accident. The current EMR systems should be complemented and improved to address problems with safe data management and medical information storage. Medical law prescribes that 'A medical expert or medical agency must make the facilities and the equipment available to create, manage and preserve EMR safely as determined by the Ministry of Health and Welfare' [6].

South Korea's Medical Law, Chapter 21-2-2, states that medical personnel or the founder of medical institutions should possess the proper facilities or equipment to protect and preserve EMRs [6]. Enforcement regulations contained in medical law and Ordinance 18 also prescribe that individual medical institutions should be equipped with a backup storage system that is disconnected from the network to keep medical records safe. Each medical agency must have the backup saved system which is not connected to a network to manage and preserve EMRs safely. The backup system is disconnected from the network for the protection of patients' personal information and medical records from third parties. Although the intent of this requirement is clear, it is practically difficult to implement the above medical laws and ordinance because of the challenges in maintaining a disconnected backup system that can store medical information accurately and quickly.

In this study, we propose six scenarios for EMR backup system using a SWOT (strength, weakness, opportunity, and threat) analysis to search for and evaluate an effective scheme.

II. Methods

A data storage and a management system are divided into 'centralized' and 'distributed'. We researched the backup policies and its methods for medical institution information system which is using in from "tertiary medical institutions" to "primary medical institution". Then, we designed six kind of backup scenarios for electronic medical records in risk management and secure data storage.

1. Backup Policy According to System Type

To manage and protect data in an information system, such as order communication system (OCS) or EMR, a backup system policy should be established as follows [7]: first, the policy should define targeting data for backup; second, it establishes a backup schedule and an interval for data storage; and third, it checks the size of data that will be stored in the backup system. Backup cannot be longer to be considered as an option, as it is essential for restoring data damaged or lost by an unexpected event. We investigated current backup systems according to the type of medical institute using the system.

Tertiary medical institutions (general hospitals/university hospitals, with more than 200 beds) manage supporting data automatically through a backup server and backup software. A backup system policy is established for two systems, one an operating system and the other a database/file system. For the operation system, the disk and duplication method of a network are used to prevent the loss of data. In this system, the operating states of the database and hardware as well as the response time of the web server are monitored in real-time, and database information preserved in the backup server is supported daily by a tape or a disk. Secondary medical institutions (30-200 beds) backup data through backup servers with support from electronic chart development by traders.

Forty-two percent of primary medical institutions (agency having beds less than 30) are backed up daily with the support of electronic chart developing traders, and 14.8% are backed up once or twice a week. No backup of data occurs in 14.4% of primary medical institutions, raising serious con-

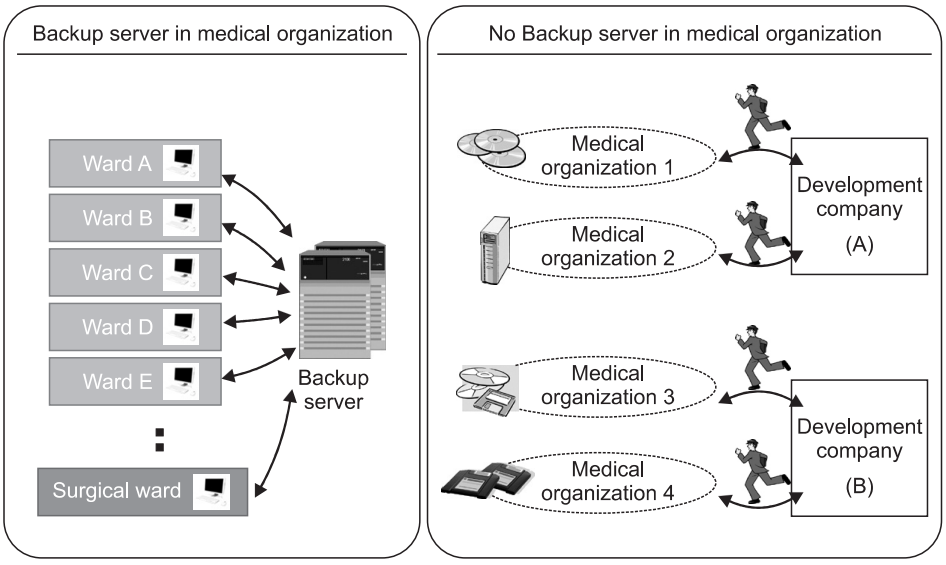

Figure 1. Independent backup by medical organizations.

cerns about the potential-loss of data [8].

2. Backup Scenarios of EMR According to Backup System Type

1) Distributed type: independent backup system by medical organizations

This type of backup system varies depending on the possession of a backup server. Medical agencies with their own backup server update their own data, whereas institutions without their own backup servers get backup service provided periodically by an outside agency (Figure 1).

2) Distributed type: self-regulated personal independent backup system

In this type of system, a patient's personal medical information is stored in a mobile medium such as a smart phone [9]. Data can be read from and recorded to the smart phone during medical examinations and treatment through a card registering apparatus at the medical institution (Figure 2). Individual patients can also store their health information in their personal computer as a back-bone.

Figure 2. Personal independent backup.

3) Centralized type: centralized backup system by the government

One of type of centralized backup system would be controlled by the central government. A backup center supervised by the government would receive the contents of medical records from all medical institutions, and would send information linked by localities or regions over the Internet. The central government would control the system that integrates these medical records and all recorded medical information [10]. This type is similar to the National Education Information System (NEIS), which is currently operating in the field of education (Figure 3).

4) Centralized type: centralized backup system by private enterprises

A second form of centralized backup entrusts backup to a third party. This enterprise possesses a large-scale data center similar to an Internet Data Center (IDC) that would provide a virtual backup system (Figure 4).

5) Hybrid type: cooperative backup system among medical organizations

The network type backup system is a hybrid method for pro-

http://dx.doi.org/10.4258/hir.2011.17.3.162

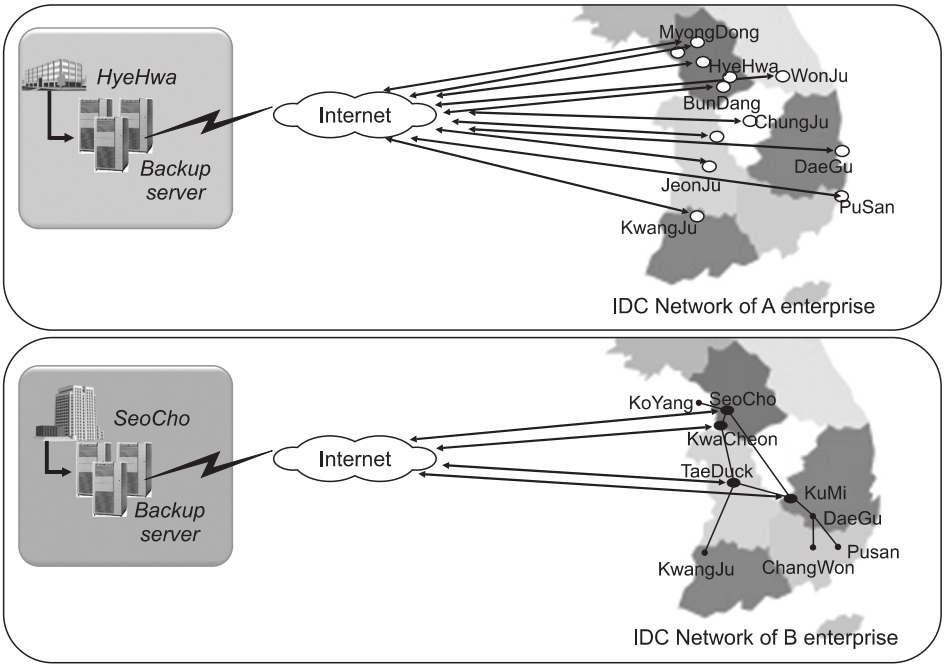

Figure 3. Central backup by the government. IDC: Internet Data Center.

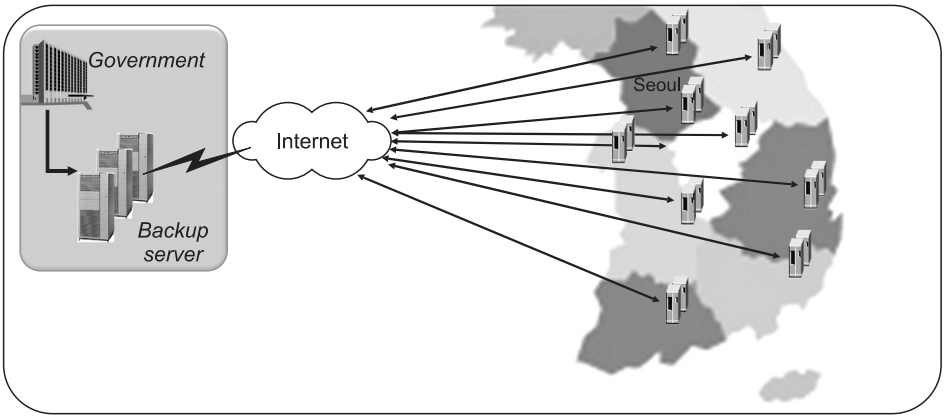

Figure 4. Central backup by private enterprises.

viding data backup. This type of system requires a cooperative network among medical institutions to jointly manage a backup center (Figure 5). Medical agencies already possessing a backup system cooperate with institutions lacking such a system so that all patient information can be secured.

6) Hybrid type: Cooperative backup system among medical organizations

In this system, data support is provided based on the individuals' trust of organizations such as the government, medical institutions, enterprises or other organization agencies (Figure 6). This concept closely resembles the Personal Internet-worked Notary and Guardian (PING) project [11,12] of the USA Children's Hospital, a program that was designed for the purpose of generating patient-centered EMRs. The basic architecture of PING consists of databases that store the PING records and a server that controls access.

III. Results

In this study, we propose an appropriate backup architecture that should support electronic medical record systems in specific medical fields. To achieve this, we analyzed the two different types of backup systems, 'centralized' and 'decentralized/distributed,' that are currently used in major information systems. We derived a decision making model to determinate a safe backup system for electronic medical records (Figure 7). We should make a decision main two things. The first decision is a structure of the backup system. To make a decision, we analyzed the general backup system such as 'individually constructed' and 'central-type constructed' with additional 'link-type constructed' backup system. The type of the individually constructed or the case-by-case constructed backup system can be divided whether it is operated by organizations or individuals. The type of

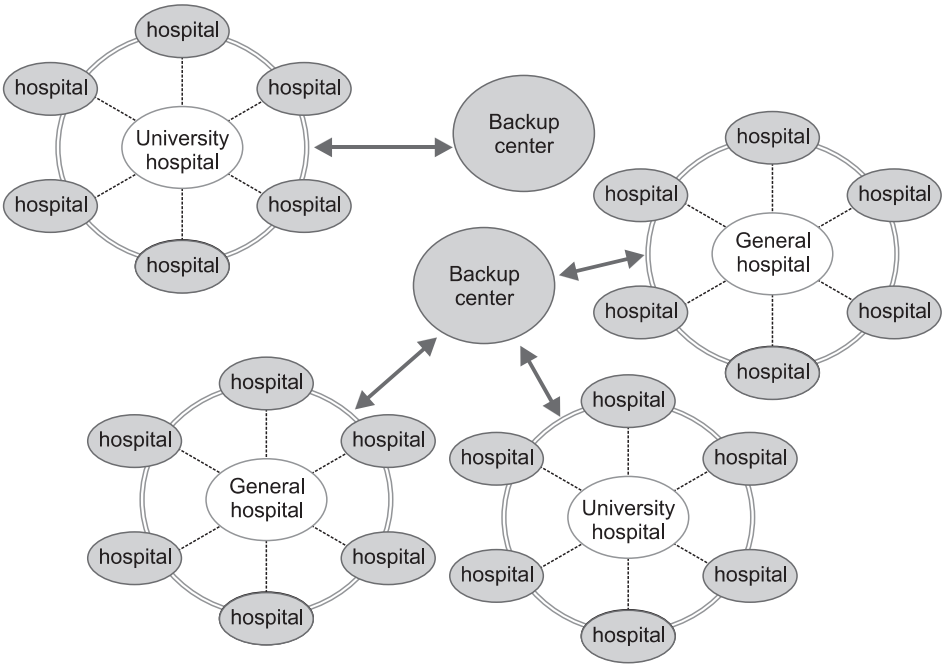

Figure 5. Cooperative backup among medical organizations.

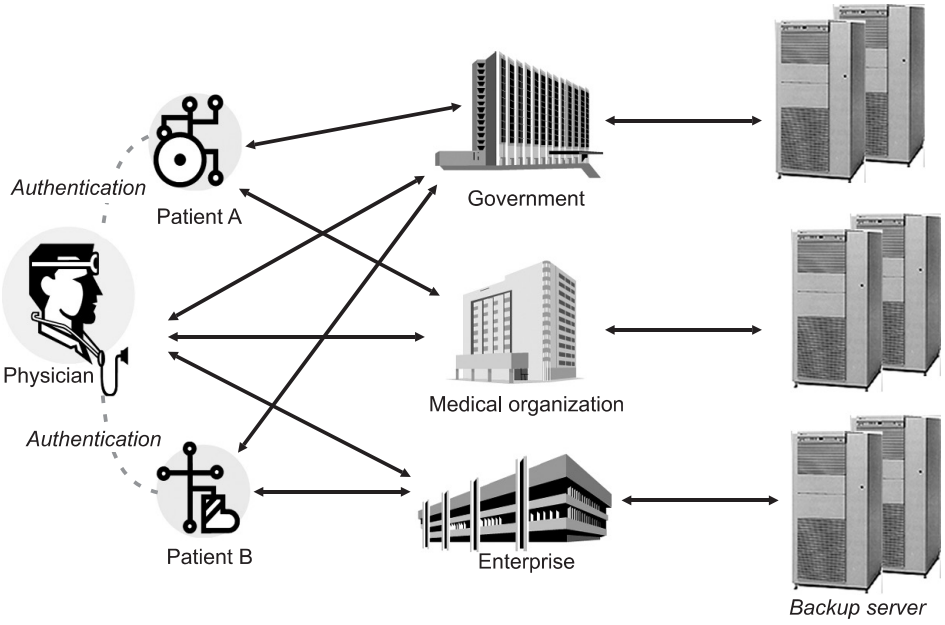

Figure 6. Backup based on mutual trust between individuals and organizations.

the central-type constructed backup system can be divided whether it is operated by the government or private enterprises. The type of the link-type constructed or the connective constructed backup system can be divided whether it is cooperated among organizations or cooperated between an individual and an organization. The second decision is who the main operation of the backup system is. It can be an individual or a medical organization.

1. Decision Making 1a: Individually Constructed Form

At present, the most common backup type in use by medical institutions is the 'independent backup system by medical organizations'. This type of system was developed in the 1990 and presents the important feature of this type of backup system that its high reliability in maintenance and recovery. However, it presents difficulties for a comprehensive backup policy, because of the varying requirements of different users. And such system lacks flexibility is also one of an obstacle for its expansion. Although backup systems can be individually constructed within particular medical institutions, the possibility of outflow of medical information is not reduced. The purpose of a supporting backup

http://dx.doi.org/10.4258/hir.2011.17.3.162

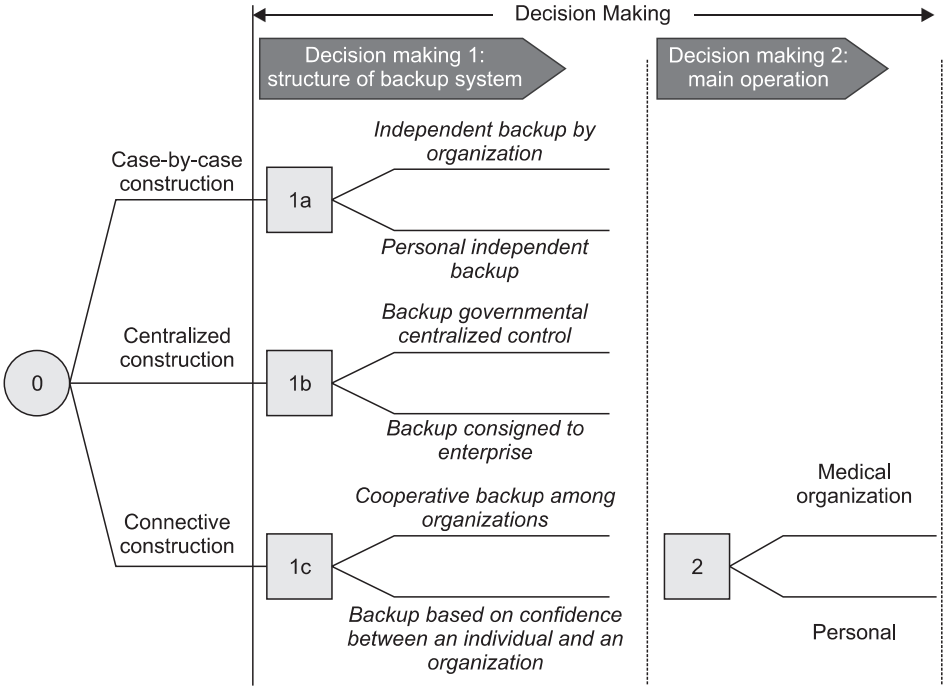

Figure 7. Model of decision making for backup scenarios.

Table 1. Decision making 1a: case-by-case construction

Case-by case construction	Strengths	Weaknesses
Independent backup by medical organization	Unparalleled reliability of security and recovery	High initial cost from absence of infrastructure High maintenance cost for employing professionals and backing-up huge amounts of data
Personal independent backup	Prevention of loss and theft of information	Risk of losing movable media and marginal capacity of media Not continuous and safe service, weak in data recovery

system for medical information is to protect data from loss or damage. Facilities, equipment and professional manpower are necessary to protect original medical information stored independently in individual medical institutions. However, as not every medical institution can maintain such facilities, equipments and human resources, an efficient management system is also needed (Table 1).

On the other hand, a 'personal independent backup system' presents a high risk of loss and a limited capacity for backup. Such a system is less likely to provide stable service without shutdown during recovery from disaster. In a 'personal independent backup' system, individual patients store their own medical information in a mobile medium, such as a smart card. Smart cards are an important way of storing patients' medical information safely. However, medical information should be kept in safer locations, such as personal computers (PCs) and personal digital assistants (PDAs).

2. Decision Making 1b: Centralized-Type Structured Form

Centralized backup systems can have robust management structures, an attribute that can reduce time and cost. A backup system constructed by the government could ensure that the protection of medical information and continuity of medical treatment in case of national emergencies, such as a war and terrorism, or disasters, such as, earthquakes, floods and fires.

A centrally controlled system gathers all information and strengthens decision making, but such monopoly of information leads to harmful effects. This type of backup system has a high risk of hacking and infringement of privacy, and it should be avoided for safe preservation of EMR. Backup systems run by private enterprises, however, have support from professional backup services and have the advantage of low management costs because they utilize previously-constructed infrastructure. Most enterprises use of IDCs, which

provide professional and cost-effective service. Many IDC companies secure users that require maintenance and attract clients. However, IDC companies currently have difficulty to securing the voluntary participation of medical institutions because they do not have legal support, whereas the general enterprise does. Systematic legal provisions for the care of medical record information should precede the involvement of private enterprises because of the risk of exposing private information contained in EMRs (Table 2) [13] .

3. Decision Making 1c: Link-Type Structured Form

The advantage of the 'cooperative backup among medical organizations' system, in which data for affiliated medical institutions are managed jointly, is that it can make data backup feasible for small-scale medical institutions. By avoiding overlapping costs, the cost of investigation and cooperative construction for backup facilities can be met. Cooperative backup systems can be formed relatively easily in the present medical regulatory environment permitting medical regulations to deal with medical information. As this type of backup system is operated with in the medical institutions, it has the advantage of relieving the privacy fears of medical institutions and users compared to the individual or centralized backup methods. However, agreement is required between the medical institutions requesting backup and those supervising the backup systems. Backup systems based on mutual trust between an individual and an organization, like the PING record managing system, are very stable and have future oriented structures. Backup systems decentralized with in a reliable organization offer a low risk of infringement of privacy and are stable from disaster. These systems only admit agents who want to reach personal backup information, and the individual will have the responsibility of approval. Thus, this type of backup system will encourage a consumer-centered medical environment [14]. However, public or private institute besides medical institutions should establish stable system first before the infrastructure is developed for individuals (Table 3).

4. Decision Making 2: Subject of Backup Operation

When a medical agency is the subject of a backup operation, it gains reliability and technical services from the backup. However, the cost burden of the medical agency is can be large in such cases. A medical agency can maintain independence to data, and the chance may arise for continuous profit creation for a person handling medical information. Legal

Table 2. Decision making 1b: centralized construction

Centralized construction	Strengths	Weaknesses
Backup under governmental centralized control	Avoids waste factors associated with construction of individual backup systems for each medical organization Saves time and investment expenses	Risk of hacking and privacy drain due to integrated management of personal medical information
Backup consigned to enterprise	Enterprise's professional and systematic backup service Low initial cost through use of existing infrastructure	Requires high-powered technology for construction of a security system Possibility that data can be used for the enterprise's profit Difficult to encourage medical organizations to participate spontaneously

Table 3. Decision making 1c: connective construction

Connective construction	Strengths	Weaknesses
Cooperative backup among medical organizations	Chance to provide backup services for small-scale medical organizations thatdo not have enough money for independent investment Prevent theft of information	No relevant legislative bill that supports this method
Backup based on confidence between an individual and an organization	Prevent theft of information Provides stable planning against calamity	High cost for individual's information backup Necessity to examine simplicity of system construction and make a long-range plan

http://dx.doi.org/10.4258/hir.2011.17.3.162

policy should be supported that enables medical institutions to become the subject if data backup operation.

On the other hand, when an individual is the subject of such an operation, the risk for exposure of medical information is relatively low. However, when medical information is released by accident, restoration measures may be insufficient (Table 4).

An owner of medical information only grants data access the specific person who gave the right approach for backup based on the mutual trust between an individual and an organization. Therefore, this system excels in personal information protection. In this system, each medical agency has to build related infrastructure. Reducing personal cost by approving only large scale enterprises that provide basic infrastructure and give limited access to patients' information in case of emergency would allow physicians to make accurate and prompt diagnosis backup based on the mutual trust between an individual and an organization. This type of system is excellent for protection of personal information, as only specific personnel approved by the medical information's owner, such as physicians, are allowed to access the information. However, infrastructure for medical institutions should be constructed separately, as the cost of using the system can be a burden for the user and also has presents limitations with respect to accessing information without personal approval in case of emergency.

We have to prevent the formation of a backup center industry that is crowded with many small-scale of enterprises, as allowing only large-scale enterprises will generate the ability to provide the required fundamental infrastructures. If some of the cost can be covered by insurance and also if the capability of reaching medical information is ensured, the burden of cost can be reduced for individual businesses and also for those who wish to perform research on data backup. In case of emergency, such a system would also facilitate prompt and accurate diagnosis of patients by doctors (Table 5).

IV. Discussion

Recently, investigation into medical informatics in medical institutions has increased, and the introduction of information systems in medical institutions has expanded, allowing improved work convenience and patient treatment. Reliance on information systems for medical work has increased simultaneously with the appearance of factors threatening uninterrupted management of information systems including viruses in computer, various limitations of information systems and human or natural disasters. Maintenance and repair of information systems in medical institutions are therefore regarded as important functions for informatics [8].

Preparations against information system disasters were very limited before the 9/11 terror attacks occurred in the US in 2001. However, once an accident occurs domestically or abroad, preparation for disaster becomes mandatory rather

Table 4. SWOT analysis of cooperative backup center among medical organizations

Strength	Weakness	Opportunity	Threat
A medical organization is able to integrate and manage the backup center systematically A medical record is secure form theft and abuse of information	Initial cost is high because of absence of infrastructure Maintenance cost is also high for employing professionals	Application of medical insurance charge Medical informatics project	Initial cost burden Risk for management of data in other hospital in cooperative

Table 5. SWOT analysis of backup center based on confidence between an individual and an organization

Strength	Weakness	Opportunity	Threat
Reliable system where an individual and an organization coexist Backup of huge amounts of data An improvement in quality of service due to competition among organizations	Precedent construction of information management system (like PING) between an individual and an organization is necessary Necessity to examine simplicity of system construction and make a long-range plan	Easy cooperation with a government agency Money for security and certification	Legal issues (whether an individual can be a main or not, whether backup to public/private organization is possible or not) Exposure of medical information to public/private organization

than elective. At present, every organization practices various backup policies to protect data against disaster. These include various measures to secure the physical storage medium, either tapes or disks, to create a real backup system by establishing a center for recovery from disaster. Distributed physical storage costs less but holds the risk of losing data created between the time when the backup was updated and the occurrence of a disaster. In contrast, real-time backup measures have the disadvantage of costing too much for feasible construction and management. Thus, every institution should choose proper measures for prevention and recovery from disaster [15]. The model medical institutions for cooperative centralized backup systems are medium and large hospitals. These institutions have the obligation to manage and preserve medical information but also possess facility and network resources and affiliated local clinics with which they can construct a cooperative network and jointly manage a centralized backup system. Cooperative medical institutions can increase their efficiency, thus increasing the quality of medical service and providing convenience for the patient. A policy that can induce medical institutions to participate voluntarily in cooperative networks is therefore necessary. A plan for creating an affiliated backup system includes the following: 1) expansion of businesses accompanying medical cooperatives, 2) admission of health insurance expenses associated with the use and storage of EMRs, 3) support of economic and legal systems that favor the construction of an efficient backup system.

The expansion of for-profit businesses with non-profit cooperatives poses problems in that the purposes of such business may be at odds with those of non-profit organizations. The 'business of medical informatics' cannot affect the treatment given by medical experts or the medical utilization of the patient. Approval of revisions to regulations to enforce this ideal is considered optimistic. Research has not yet found a way to create stricter regulations for business supporting medical cooperatives, although such regulations exist for educational or social welfare cooperatives.

For the safe preservation of EMRs policies that will encourage medical institutions to participate in affiliated backup systems, such as allowing expenses to be covered by insurance, are necessary. A medical image storage and transfer system called picture archiving and communication system (PACS) was installed and began operating in Samsung Seoul Hospital, a large scale hospital, in 1994. PACS was also installed in Bundang Jaesaeng Hospital, which opened in 1998, and in Ilsan Paik Hospital, which opened in 1999. The spread of PACS was subsequently accelerated in Korean hospitals because X-ray examination and reading through PACS have been covered by medical insurance since the end of 1999. PACS, which includes diagnosis storage, management and search functions, has proven to be very useful and economically valuable, increasing the speed of medical examination and treatment, the productivity of the hospital and the scale of the hospital [16].

Medical regulations for the management and storage of EMRs define backup with safe management and preservation obligatory. However, remote control of backup is not permitted. Legal support for remote backup is necessary in terms of detailed prescriptions of range and safety standards [6] (Figure 8).

If EMR information was linked to a network, every person connected to the network could potentially have access, increasing the possibility of medical information being disclosed to a third party. If a third party were to penetrate the network illegally, the damage would be expanded. However, the disadvantages of banning network-linked backup systems should also be taken into account. If a backup system was not linked to the network and thus medical information was not automatically backed up, users would have to complete extra storage processes and incur additional expenses. Data could be delayed, information could be omitted and information could be corrupted during the storage process. Such a scenario would threaten the reliability, stability, and efficiency of the backup system.

Stored medical information, as defined in Medical Law Chapter 21-2-3, is equivalent to EMR. If stored personal information is stolen, spilled, altered or damaged, then

Chapter 18-2 (equipment necessary for preservation of EMR)

Chapter 21-2-2 medical personnel or the founder of the medical institute should prepare to safely manage and preserve EMRs using the following;

1. Apparatus that can verify formation of EMR and electronic sign.
2. Apparatus that can confirm alteration of EMR after electronic sign is done.
3. Backup storage system that is not connected to the network

[Professional revision 2003.10.01]

Figure 8. Medical regulation (Chapter 18-2).

http://dx.doi.org/10.4258/hir.2011.17.3.162

Medical Law Chapter 66-3 dictates a punishment of imprisonment of 5 years or a penalty of less than 20 million won. Stored medical information will therefore be protected by the above-mentioned regulation. It is pertinent that the above regulation, Chapter 18-2-3, is interpreted as banning extra-network but not ordinary intra-network transfers of information. Therefore, an intra-network backup system does not violate regulations, and cooperative backup systems for consortia among medical institutions need to be examined for a possible promotion after a thorough review for legal problems.

In this study, we proposed a plan for improving legislation as well as a solution for constructing an EMR backup system center based on advanced information processing techniques. This research implements that backup scenario such a medical institution after analysis type backup policy. Therefore, methodological analysis is limit particular not direct survey of many medical institutions.

Conflict of Interest

No potential conflict of interest relevant to this article was reported.

Acknowledgements

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2010-0028631).

References

1. Seo HJ, Kim JH. Correction system of a mis-recognized medical vocabulary of speech-based electronic medical record. J Korean Soc Med Inform 2002; 8: 11-20.
2. Davis K, Doty MM, Shea K, Stremikis K. Health information technology and physician perceptions of quality of care and satisfaction. Health Policy 2009; 90: 239-246.
3. What is an EMR (Electronic Medical Record): EHR (Electronic Health Record)? [Internet]. New York: About.com, The New York Times; c2010 [cited at 2010 May 30]. Available from: http://patients.about.com/od/electronicpatientrecords/a/emr.htm.
4. Department of Health and Human Services. The decade of health information technology: delivering consumer-centric and information-rich health care. Report to the Secretary of the Department of Health and Human Services. Washington, DC: Department of Health and Human Services; c2010 [cited at 2010 May 31]. Available from: www.hhs.gov/healthit/documents/hit framework.pdf.
5. Cheong HJ, Shin NY, Joeng YB. Improve Korean service delivery system in health care: focusing on national e-health system. In: Proceedings of 2009 International Conference on e-Health, Telemedicine and Social Medicine; 2009 Feb 1-7; Cancun, Mexico; p263-268.
6. Ministry of Health Welfare. Medical law. Seoul: Ministry of Health Welfare; 2004.
7. Yoo SY, Yu SY, Min MG. Hospital information-oriented present state research. Seoul: Research institute for Healthcare Policy; 2003.
8. The Office for Government Policy Coordination, Ministry of Information and Communication. Guideline for backup of information system. Seoul: The Office for Government Policy Coordination; 2005.
9. Sarasohn-Kahn J. California Healthcare Foundation. How smart-phones are changing health care for consumers and providers [Internet]. California Healthcare Foundaion; 2010 [cited 2010 May 20]. Available from http://www.chcf.org/~/media/MEDIA%20LIBRARY%20Files/PDF/H/PDF%20HowSmartphonesChangingHealthCare.pdf.
10. Hwang JS, Choi SH. E-governance business and personal information protection issue-centering on NEIS. Seoul: Korea Information Society Development Institute; 2003.
11. Riva A, Mandl KD, Oh DH, Nigrin DJ, Butte A, Szolovits P, Kohane IS. The personal internetworked notary and guardian. Int J Med Inform 2001; 62: 27-40.
12. Katirai H, Sax U. Unlocking the value of clinical information: what you need to do now to enjoy the benefirts in the future. Lect Notes Comput Sci 2005: 3782; 330-338.
13. Bang DH, Kim HK. Legal issue and solved theme of personal information protection. Seoul: National Information Society Agency; 2004.
14. Kim J. The comparison analysis of opinions towards the concept of consumer health informatics among Korean and American health informatics academic society members. J Korean Soc Med Inform 2005; 11: 17-25.
15. The Office for Government Policy Coordination & Ministry of Information and Communication. Guideline for Disaster Recovery of Information System; 2005.
16. Han Y, Park H. Cost-effectiveness of PACS based on medical insurance coverage. J Korean Soc Med Inform 2000; 6: 51-63.