

## Personal Information Protection Issues and Its Solutions

Seung-Il Moon<sup>1</sup>, Ki-Min Song<sup>2\*</sup>, Jae-Hun Shim<sup>3</sup> and Ho-Young Choi<sup>4</sup>

<sup>1</sup>*Hanyang University, Seoul, Korea*  
*{moonsi921,moolgatti}@hanyang.ac.kr*<sup>2</sup>

<sup>2</sup>*Hanyang University, Seoul, Korea*  
*haieung@hanyang.ac.kr* (**Corresponding Author**)

<sup>3</sup>*Baekseok University, Chungcheong, Korea*  
*clinicalpt@bu.ac.kr*

### Abstract

*This study aims to review the legal system concerning information efficiency and privacy protection on the U-Health infrastructure construction for the disabled. Regarding methodology, related provisions such as U-Health, legal definitions of the disabled, as well as Privacy Protection Act for security are analyzed and studied. As a result, Personal Information Control Right of the information agent should be secured in the gathering, processing, use and provision of the medical information. Also, legal norms to protect personal medical information leakage due to inadequate administrative and technical action are required.*

**Keywords:** *Personal Information Protection Policy, U-Health, Security, Personal Information Protection Act, Information Protection, Medical Information Protection*

### 1. Introduction

Government and local government should provide policies for the disabled including physical and mental rehabilitation services to learn or to restore their capabilities, and aids to make up for their disabilities (Article 18 of the Welfare Act for the Disabled). But a survey shows that along with the living standard security, medical issue is one of the major concerns for the disabled. Health and medical treatment system for the disabled is insufficient in Korea, and studies in this field are also meager compared to those of welfare[1].

Also, as the need for the public medical service grows from medical treatment to the improvement of the quality of life including prevention and health promotion, laws related to remote medical services and U-Health are complementary. However, legislation and application time are inconsistent that they hinder simultaneous diffusion of the U-Health. Scope of telemedicine in the Medical Act and the protection of personal information for security in the Privacy Protection Act should be improved for the activation[2].

Construction of the U-Health infrastructure, where both effective information to meet the need for medical needs of the disabled and privacy protection are harmonized, is required.

This study is a basic research to present security issues and solutions concerning personal information protection in U-Health for the disabled. Definition of U-Health and the disabled, and provisions in the Privacy Protection Acts of Korea concerning security are interpreted, analyzed and studied.

## **2. Theoretical Backgrounds**

### **2.1. U-Health**

U-Health, abbreviation of the ubiquitous health, is a medical service which provides prevention, diagnosis, treatment, and follow-up care without visiting doctor at anytime and anywhere. With the development of the medical technology, it has advanced from the medical treatment and follow-up care to the prediagnosis and prevention of the diseases, and it widens the scope of the concept including enhanced quality of medical services and sustainable healthy life. U-Health, abbreviation of the ubiquitous health, is a medical service which provides prevention, diagnosis, treatment, and follow-up care at anytime and anywhere without visiting doctor. With the development of the medical technology, it has advanced from the medical treatment and follow-up care to the prediagnosis and prevention of the diseases, and it widens the scope of the concept including enhanced quality of medical services and sustainable healthy life.

### **2.2 Disability**

In Korea, disability is a term covering the physical or mental impairment. Welfare of Disabled Persons Act defines the disabled as an impairment or loss of physical or mental functions that substantially limits an individual's personal or social activities for an extended period. Such a general definition is called a Medical Model for Disability or Rehabilitation Model. In Korea, legality of the disability is defined and limited by medical model requirements (Japan and Korea adopt this among the OECD countries). The category of the disabled was restricted, but ongoing expansion includes internal organ impairment and partial social disabilities (for example, facial disorder). With the expansion of the legal disability category, and with the increase of the traffic accident, industrial accident, and ageing, the disabled population is expected to grow. And in fact, the disabled population in Korea continues to increase.

### **2.3 Privacy Protection of the Personal Health (or Public Medical Services) Information**

#### **2.3.1. Personal Health (or Public Medical) Information**

Personal medical information is a very sensitive issue, but its proper use for the advancement of medical service or public health also should be considered [3]. On the other hand, though the secondary use of the personal medical information may contribute to the medical services, careless misuse would invade privacy, diffuse negative recognition, and consequently hinder studies and development by the secondary use. Therefore, both active secondary use of the personal medical information and privacy protection should be considered. It includes the protection from the government as well as from the private body.

#### **2.3.2. Personal Information Protection Policy**

As the information society advances, and as the economic value of the personal information increases, gathering and use of personal information is generalized in every aspect of the society. However, because general principle for the protection and use of the personal information is not yet prepared, it has blind spots for the personal information protection, and causes privacy violation including leakage, misuse, and abuse of the personal information. And it results in mental and financial damage by privacy violation, an illegal name use, voice phishing. For the protection of the privacy, rule for personal information processing to meet the international standard both in the public and private sector should be defined, and national relief scheme for the privacy violation should be

reinforced. For the rights and benefits protection of the personal information, Personal Information Protection Act was established on the 29th March, 2011, replacing Protection of Personal Information in a Public Institution Act.

The information protection act protects 'personal information'.

According to Article 2 (1) of the same Act, "personal information" is information on a living individual and refers to information that can identify an individual through name, resident registration number, and video (Even if a specific individual cannot be identified based solely on that information, it includes something that can be easily combined with other information for identification). Conversely, it is not personal information that 'is easy to combine with other information', but does not recognize a particular individual or 'is able to recognize a particular individual only through combination with other information that is very difficult. In other words, 'ease of combination' and 'possibility of identification' are conceptual elements.

After the first revision in December 2013, the Ministry of Health and Welfare and the Ministry of Government Administration and Home Affairs revised it secondly to the 「Guidelines for Personal Information Protection - Medical Institutions」 in February 2015. In 2015, on the other hand, the Ministry of Science, ICT and Future Planning published 「Guide to Utilization of Personal Information De-identification for Big Data Utilization」. Also, on June 30, 2016, the Office of State Coordination, the Ministry of Government Administration and Home Affairs, the Korea Communications Commission, the Financial Services Commission, the Ministry of Science, ICT and Future Planning, the Ministry of Health and Welfare jointly announced the 「Guidelines for Personal Information De-identification Action – Guide to Criteria for De-identification Action and Support and Management System-」. However, the above guidelines are not legally binding as a kind of administrative rule established without the delegation of law. Moreover, the National Human Rights Commission of Korea expressed its opinion that Section 2 Item 4 of Article 32 (2) and Section 7 of the same article of 「Some amendments to the Act on the Use and Protection of Credit Information」 announced for legislation on April 20, 2016 by the Financial Services Commission may violate the right to self-determination of personal information by allowing credit information companies to use de-identification information for other purposes with the consent of the credit information entity or to provide it to third parties, so it is necessary to clarify the concept of de-identification measures and strengthen requirements, restrict use and offer for the purposes of other than the purpose of de-identification information, restrict the third party scope provided with de-identification information and complement measures for prevention of re-identification of third parties and safety measures for re-identification information.

### **2.3.3. Personal Information Protection and U-Health**

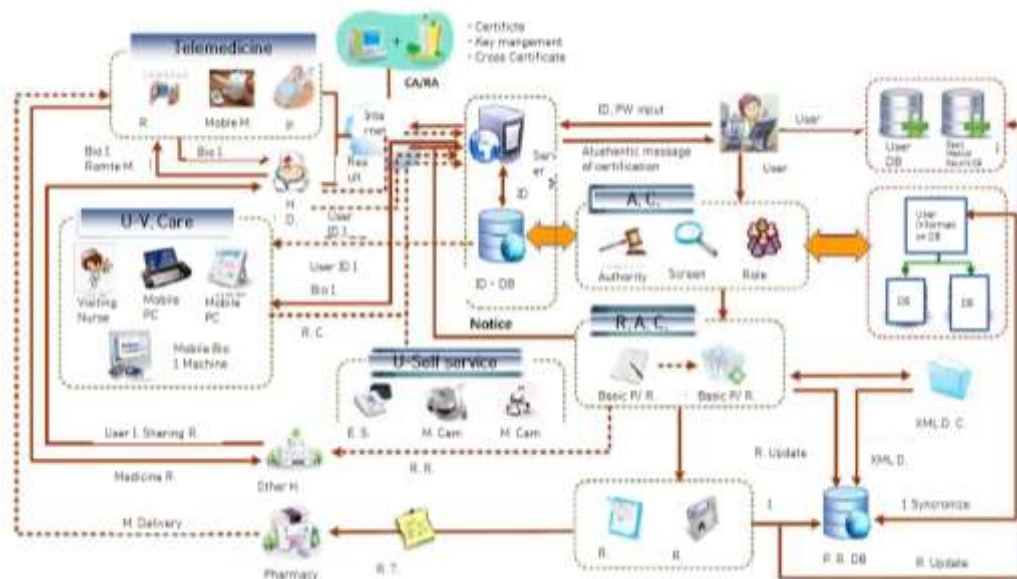
U-Health care service requires medical information exchange and sharing between related organizations and users so as to promote the BINT technology fusion as well as to provide more correct and various medical services. There is more serious concern for security, because U-Health care service handles very sensitive information comparing to other ubiquitous computer technology and various domains or service partakers share information.

The establishment of a u-healthcare infrastructure for the disabled requires a harmony between effective information and privacy protection to meet the needs of people with disabilities. Therefore, various security issues and reasonable alternatives must be fully considered to expand highly reliable u-health care services.

Therefore, various security issues and reasonable solutions should be concerned in order to promote reliable U-Health care services[4].

The above de-identification of personal information is presented as an alternative, but has not been properly settled yet. In this regard, Japan's 「Act on Personal Information Protection(個人情報の保護に関する法律)」, enforced on September 9, 2017 (Pyeongseong 27), has a great significance. The same act introduced the concept of 'anonymous processing information'. Anonymous processing information is the information on individuals obtained by processing personal information to prevent a specific individual from being identified by taking action such as 'to delete a part of the description 40) included in the personal information (Including replacement with other descriptions in a way that does not have the regularity to restore some descriptions)' or 'to delete all of the personal identification codes included in the personal information (Including replacement with other descriptions in a way that does not have the regularity to restore the personal identification code)' etc., (Article 2 (9) of the same Act). Distinguishing between those who write anonymous processing information and those who handle anonymous processing information, the same act added considerable duties to each subject.

That is, it newly established regulations such as the obligation to create unrecoverable information, the duty to prevent information leakage, the obligation to disclose information items, the obligation to disclose and express when providing the information to third parties, the obligation to prohibit discrimination, the obligation to take safety management measures those who write it and the obligation to disclose and express when providing the information to third parties, the obligation to prohibit discrimination, the obligation to take safety management measures for those who handle it. Solving the de-discrimination, it is to think about practical efforts to minimize the echo, and to incorporate it into legislation. An example of a u-healthcare service model that can securely access personal information of the disabled according to the authority when the personal information of the disabled between institutions such as hospitals is requested by integrated management of the IDs used by users in the u-healthcare environment is as follows. The proposed model consists of functions such as user identification, institution authority confirmation, medical record access control, and patient diagnosis for effective use in a real environment.



[Figure] A Suggested Model for User Privacy Assurance

### 3. Research Findings

The use of personal medical information concerning U-Health of the disabled should be expanded beyond the medical institution, and should be promoted as an industry. Therefore, legislation and revision concerning medical information protection are required as follows.

First of all, personal information control right concerning gathering, process, use and provision of medical information should be guaranteed. Comparing Medical Act and Privacy Protection Act, privacy protection and access right to read and copy personal information is restricted. Therefore, right to correct or delete medical information and right to express one's objection should be reflected.

Secondly, free distribution of medical information should be guaranteed. As the processing environment of the medical information (especially, increase in medical information use and medical institution) changes, clauses for the use and provision of medical information should be regulated by detailed legislation and radical changes in legislation contents and method are required. New legislation (Medical Information Protection Act) would be required in order to promote healthy development of medical information industry and to regulate procedures for use and provision of medical information[5]. Like Japan's 「Act on Personal Information Protection(個人情報保護に関する法律)」, worries and plans such as the distinction between the de-discrimination writer and the handler should be legislated in addition to the de-discrimination measures.

Thirdly, legal criteria for the personal medical information leakage by incomplete administrative and technical action are required. Article 29 of the Information Protection Act guarantees 'safeguard duty' stipulating that "personal information processor should take technical, administrative and physical measures following the executive order, including internal management plan, and access records storage to secure personal information from loss, robbery, leakage, falsification or damage." However, as the medical network system between medical institutions is not same, technical and administrative measure is not easy and standardization would be unsuitable. Furthermore, even when the medical institution doesn't take measure due to financial or other reasons, regulation cannot be urged[6].

**Table 1. Decree and Major Actions-Guidelines for the Personal Information Protection in the Medical Institute**

	Medical Information	Personal Information
Concept	<ul style="list-style-type: none"> <li>○ Information including personal information for the medical treatment</li> <li>- Medical Records, Operation Records, Immature Labor Records, Patients Records etc.</li> </ul>	<ul style="list-style-type: none"> <li>○ Member Information on the Web, Personal Information including contact information for promotion</li> </ul>
General Principle	<ul style="list-style-type: none"> <li>○ Priority of Medical Act</li> <li>Otherwise, application of the Personal Information Protection Act</li> </ul>	<ul style="list-style-type: none"> <li>○ Application of the Personal Information Protection Act</li> </ul>
Collection and Use	<ul style="list-style-type: none"> <li>○ Article 22 of the Medical Act(Clause 14 of the Regulation)</li> <li>- Collectible without agreement</li> <li>- Limited to the medical purpose</li> </ul>	<ul style="list-style-type: none"> <li>○ Article 15 of the Personal Information Protection Act</li> <li>- Collectible with agreement</li> </ul>
Management	<ul style="list-style-type: none"> <li>○ Personal Information Protection Act</li> <li>- Article 26 : Written commission and its public acknowledgement should be notified.</li> <li>- Article 29 : Protection measurement including access control, data</li> </ul>	

	<p>encryption, access record keeping, physical protection measurement should be certified.</p> <p>- Article 30 : Personal information protection policy should be established and open to public.</p> <p>- Article 31 : Person in charge of the personal information protection should be appointed.</p>	
Provision and Reading	<p>O Article 21 of the Medical Act - Provision and reading is not allowed if not designated by the Medical Act*. * Request of family or a legal representative, special regulation</p>	<p>O Article 18 of the Personal Information Protection Act - Provision and reading is not allowed except designated by the Personal Information Protection Law.* * Allowed with the presentation of other legal basis</p>
Process of Request including Modification and Erasion	<p>O Article 22 of the Medical Act - Modification and Erasion of legal information is not allowed.</p>	<p>O Article 35 and 36 of the Personal Information Protection Act - Request for the reading, modification and erasion of the person concerned should be allowed, unless restricted by laws.</p>
Storage and Destruction	<p>O Article 15 of the Medical Act - Legal minimum holding period should be obeyed, and extension is allowed if necessary for the medical treatment.</p>	<p>O Article 21 of the Personal Information Act - Immediate destruction after use</p>
Transfer	<p>O Article 40 of the Medical Act - Transfer of medical information to the head of local health center concerned, in case of permanent or temporary closure. - Storage by the medical institute founder is allowed, if permitted by the local health center head. ※ Change of the permitted fact is regarded as the maintenance of the medical institute.</p>	<p>O Article 27 of the Personal Information Protection Act - Change of the medical institution should be notified to the person concerned.</p>
Act against Leakage and Violation	<p>O Article 34 of the Personal Information Protection Act - Leakage should be notified to the person concerned and should be reported to Ministry of Public Administration and Security or specialized agencies(KISA, NIA) if exceed 10,000 cases. O Article 62 and 63 of the Personal Information Protection Act - cooperation with the investigation, if the person concerned reports information leakage to the report center.</p>	
Operation of Visual Information Process Facilities	<p>O Article 25 of the Personal Information Protection Act - Signs to notify the CCTV installation in the public space as waiting room should be installed. O Article 15 of the Personal Information Protection Act - Contentment of the people concerned is required, if CCTV is installed private spaces as consultation room and operating room.</p>	

The Health Insurance Review & Assessment Service provides 'Self-Checking of Personal Information for Medical Institutions' service from August 2015, so that the medical institution can understand and comply with the Personal Information Protection

Act. This service helps to make up for missing things by autonomously identifying the personal information management status of each medical institution. From April 12, 2016, 'Self-Checking Guide by Self-Check item of Personal Information Protection of Medical Institutions' is provided through work portal system for medical institutions. As shown above, their own technical and administrative measures should be taken through the Health Insurance Review & Assessment Service, the 'Korea Disabled People's Development Institute' (Article 29, Clause 2) under 「Welfare of Disabled Persons Act」.

#### 4. Conclusion

With the actual application of telemedical service such as U-Health care, medical service would not be provided in stationary positions. Relative instrument and system including home medical devices for telemedicine, mobile medical devices, electronic prescriptions, information of medical institutions, clinical information sharing, information application system for personal disease management, provision of health-related contents should be developed[7].

Though technical, managerial, and physical treatment is legally required, its execution is not mandatory. Installation of data server among the infrastructure mentioned, for example, is possible in the large medical institution, but it can be a financial burden for the smaller ones. Therefore, with the generalization of IDC(Internet Data Center) and cloud computing, insertion of provisory clause to substitute data server to web hosting should be considered.

Concerning the distribution of medical information, specific regulation should be established. Reading and use of the patient's medical history information should be restricted to limited persons (medical doctor, and protector of patient, minor, quasi-incompetent, or incompetent) in order to secure privacy. Specific definition for medical information should be given, range of knowledge for the public medical services within the Framework Act on Health and Medical Services should be specified, and the notion of accessibility should be stipulated[8].

#### References

- [1] B. S. Lee, " Health Care Delivery System for Disable Person and Medical Market Opening among Advanced Countries". Fountain of Rehabilitation. Vol. 18. (2005).
- [2] T. M. Song, et al. "u-Health: Current Status and Tasks Ahead", Seoul: Korea Institute for Health and Social Affairs, (2011).
- [3] J. Y. Park, "Analysis of Legal Basis Regarding Patient Privacy and Protection of Information". Korean Journal of Medicine and Law, Vol. 20, No. 2, (2012), pp.123-143.
- [4] J. E. Song, S. H. Kim and M. A. Chung, "Medical Information Security in u-healthcare service". KIISC REVIEW. Vol. 17, No. 1, (2007), pp.247-271.
- [5] D. H. Hyeon, "Consistency of Personal Data Protection between Personal Data Protection Act and Other Acts. in Direction of Personal Information Protection Policy in Personal Data Protection Act", Seoul: Korea Internet Law Association and Korea Internet Security Agency, (2016).
- [6] H. J. Lee, "Problems and Solutions of Personal Information Protection in the Medical Area". Korean Journal of Medicine and Law. Vol. 20, No. 2, (2012), pp.158-172.
- [7] D. S. Jang, "Medical Information on u-healthcare environment". Korea Information Processing Society Review. Vol. 15, No. 1, (2008), pp. 55-68.
- [8] Y. H. Yoon, "Enhance Issues of the global competitiveness of Telemedicine Industry in Korea", International Commerce and Information Review, Vol. 13, No. 3, (2011), pp. 325-351.

## Authors



**Seung-II Moon**, is a professor of Hospitality Academy in Hanyang University. He has a lot of interest in IT, information and Multidisciplinary. He has written many papers and books on these fields and given lectures for years. He worked as a webmaster and Internet honorary national police officer.



**Ki-Min Song**, is a professor of Hanyang University and Director of R&SD Strategy Center. He has a lot of interest in Medical and Convergence industry. He has published many papers of these fields and given lectures for years. He received bachelor's and doctor's degrees in Hanyang University.



**Jae-Hun Shim**, is a professor of Baekseok University. He has a lot of interest in Public Health New Product, IT Service Development, Learning Technology, related problem-solving (Medical Technology). He received doctor's degrees in Hanyang University.



**Ho-Young Choi**, is a director of Health Insurance Review & Assessment Services. He worked in the area of U-Health. He received a Master's degree in Seoul National University.