Security Requirements for the Medical Information Used by U-Healthcare Medical Equipment

Jaebum Son[1], Soonseok Kim[2], Gilhong Park[1], Jihun Cha[3] and Kijung Park[3]

[1]*Department of Biochemistry, College of Medicine, Korea University 126-1, Anam-dong 5 Ga, Seongbuk-gu, Seoul, 136-701, Korea*
[2]*Department of Computer Engineering, Halla University San 66, Heungup-Li, Heungup-myon, Wonju-shi, Kangwon-do, Korea*
[3]*National Institute of Food and Drug Safety Evaluation, Fusion Technology Medical Device Team, Chungcheongbuk-do Cheongwon-gun Gangoe-myeon Osongsaengmyeong 2 Ro 187, Korea*
Jaebum.son@gmail.com, sskim@halla.ac.kr, ghpark@korea.ac.kr, {woongcjh, jebipark}@korea.kr

Abstract

Home healthcare based on ubiquitous technology (u-technology) is emerging as a solution to increasing chronic disease patients with the advent of aging of society. While u-technology has the advantage that improves accessibility to medical services, it also increases the probability of the infringement of privacy of personal medical information, the leakage of which can do greater damage than any other information. At the juncture that social requirement for privacy protection is getting important, the development of standard and specification to evaluate the minimum security level of u-health medical devices is inevitable as a prerequisite for the vitalization of u-health.

This study aimed at the development of security test methodology for u-health medical devices and proposed the standard and specification to secure medical information security. For the purpose, first, we defined the scope of u-health medical devices and categorized its physical and operational types. Second, security core technologies were selected that can be applied to u-health medical device in three aspects such as administrative safeguard dealing with operator, policy, document, system and user education, physical safeguard dealing with control of entrance and exit, screen or shared instrument, and technical safeguard dealing with computer system-related technological elements. Lastly, each security core technology was assigned to each physical and operational types of u-health medical devices and relative significance of which was determined. The guideline containing the developed security core technology and test methodology for u-health medical device would be utilized for the enhancement of security level in the design of u-health medical devices and setting the authentication standard for authorization process for security in Korean Food and Drug Administration.

Keywords: *u-health medical device, medical information security, security core technology, security test methodology, authentication standard.*

[1] First author : Jaebum Son, Jaebum.son@gmail.com
[2] Corresponding author : Soonseok Kim, sskim@halla.ac.kr

1. Introduction

The current reality in which the number of patients with chronic diseases such as diabetes and high blood pressure accounts for 20% of the entire domestic population, with resultant healthcare costs exceeding 7% of the GDP, is expected to worsen with the advent of an ageing society [1, 2]. To date, a number of solutions to such concerns have been proposed. Of those solutions, u-health, a new kind of IT-based healthcare service based on the Internet or the like, can be regarded as the most promising alternative. U-health has come into the spotlight as a fresh opportunity to create a new convergence market by means of providing network-based medical and healthcare services. In particular, u-health has rapidly secured its position, along with the state-backed research support driven by the possibility that cost saving is possible without impairing the quality of services related to patients with chronic diseases [3].

However, the two key elements of u-health that is, IT and healthcare are not easily mixed with each other due to the fundamental difference in the characteristics and expertise that are needed in the two disciplines. Above all, u-health-related medical equipment and systems are deemed to be a prerequisite of u-health in the recent days, with growing privacy and security concerns corresponding to medical information, as such equipment and systems are dealing with personal health information despite the fact that they are IT systems. In effect, u-health technologies are like a double-bladed sword in that such technologies can help improve public health through enhanced accessibility to medical services, while increasing a risk of leaking personal medical information. As most of the information spreading through u-health is personal medical information or a kind of information that must be protected, the consequences of information leakage has a huge ripple effect, compared with general personal information. In this regard, the following international standards are being applied with regard to personal (medial) information: ISMS (Information Security Management System), such as ISO 27001/27799 [4-6], IEC 60601 [7, 8], the HIPAA Act in the US [9, 10], etc. The related statutes in Korea are as follows: The Personal Information Protection Act (Act No. 10465, the Ministry of Public Administration and Security) [11], the Act on the Promotion of the Use of IT Networks and Information Protection, etc. (Act No. 10560, the Korea Communications Commission) [12], the Medical Act (Act No. 11005, the Ministry of Health, Welfare and Family Affairs) [13], the Standards for Technical and Administrative Protection of Personal Information (Public notification No. 2011-01, the Korea Communications Commission) [14]. The Korea Food and Drug Administration had once established item-by-item approval and screening guidelines for u-healthcare medical equipment in compliance with the security and administrative principles stemmed from the fact that personal medical information must be securely managed according to the three information security principles - confidentiality, integrity, and availability [15]. The aforementioned three elements (confidentiality, integrity, and availability) must be understood prior to implementing any security measures regarding personal medical information, and it is recommended that technical requirements should be referred to TTAS.KO-10.0304 (the Technical Requirements for Protection of Personal Health Information) [16]. If biometric information is used for identifying users, it is recommended that TTAS.KO-

12.0034 (the Guideline for Biometric Information Protection, the Telecommunications Technology Association in Korea) [17] should be referred to. In addition, the security compliance of networks, separately connected and used by public agencies, must be certified in accordance with the evaluation standards stipulated in the Personal Information Act [18].

With growing social and systematic demands for protection of personal medical information, personal medical information of the public has become a prerequisite for the revitalization of u-health, and which security elements should be taken into account has become a the highest priority with respect to remote healthcare medical equipment (hereinafter referred to as "u-health medical equipment").

Consequently, this study has focused on drawing up a guideline by virtue of deriving security requirements for medical equipment handling personal medical information, while developing security measures for relevant information in terms of the management of all kinds of information systems (including both hardware and software) related to personal medical information, which is being used for collecting, accessing, saving, transmitting, and processing the personal medical information created from u-health medical equipment.

2. Deriving Security Items for u-health Medical Equipment

In this study, security assessment items that can be used in u-health environments and the assessment methods thereof have been developed. To achieve this, the security items suggested by existing personal information security standards and guidelines had been arranged and reinterpreted according to the u-health medical equipment categories, and then, of those items, the security items falling into the approval and screening categories released by the Korea Food and Drug Administration were selected. On the other hand, the security elements that need to be taken into account for designing u-health medical equipment are newly derived in consultation with security experts. In particular, many items were arranged by the advice of u-health medical equipment or system operation experts.

2.1. Categories and Definitions of Information Security for Medical Equipment

The security requirements for general information system comprise administrative organizations, human resources, physical elements, such as buildings and entrances. Put broadly, the administrative safeguard is concerned with the elements including policies, document systems, user training, and the like from the administrative standpoint of management u-health, whereas the physical safeguard includes the control of entrance doors, screens, shared devices, and the like, and the technical safeguard includes technical elements (*e.g.*, firewalls, anti-virus programs) related to computer systems. For medical equipment, considering the aforementioned conventional administrative and physical safeguard within the equipment category itself might be inappropriate. However, the domain of each security element has been classified and defined with

respect to u-health medical equipment, as shown in Table 1, on the basis of such a classification system.

Table 1. Categories and Definitions of Information Security for u-health Medical Equipment

Security category	Definition
Administrative safeguard	The elements that are specified in user manuals, such as handling methods, precautions, countermeasures against security breaches that may be caused by the problems of medical equipment, in order to lower the risk of a security breach concerning personal medical information
Physical safeguard	The elements that are exposed to the risk of a security breach concerning personal medical information or can determine the levels of security breaches due to the physical design of medical equipment
Technical safeguard	Technical security elements that are generally referred to. Esp. IT security elements.

2.2 Deriving Security Items for u-health Medical Equipment

According to the aforementioned standards, security items applicable to u-health medical equipment and falling into the approval and screening categories released by the Korea Food and Drug Administration have been gleaned by category from the following: the ISMS items specified in ISO 27001/27799 [4-6] or the like, IEC 60601 [7, 8], the HIPAA Act in the US [9, 10], related domestic statutes, the guidelines [15, 19] released by domestic official agencies, such as the Ministry of Health, Welfare and Family Affairs, the Korea Food and Drug Administration, and the like, the opinions of security and network experts, and new security items derived by researchers, etc. The grades of each security item in the following are classified into "mandatory," "recommended," and "for reference." The derived items are as follows. "O" was assigned to the common security factors and the cases in which there is no applicable security element at the moment. However, the elements that can be additionally applicable during the course of the development of related technologies are expressed as "RESERVED." (Refer to Table 2).

Table 2. Security Items and Grades for u-health Medical Equipment

Code	Security item and grade
10	U-health medical equipment: common security elements
100	Common security elements for u-health medical equipment
1001	(Mandatory) Personal health information that needs to be collected (administrative safeguard): No information, except for the items that must be collected for u-health services, shall not be collected
1002	(Mandatory) Providing technical information related to processing personal health

	information (administrative safeguard): The manuals attached to medical equipment must include clarified descriptions on how to acquire, store, transmit, and delete personal health information. The technical items here mean the following: (1) The types of data and personal health information that are allowed to be collected and how to collect such data; (2) Transmission methods (protocols, transmission conditions, transmission encryption, etc.); (3) Encryption methods, etc.
1003	(Mandatory) Clarification of responsibility in the event of a security breach (administrative safeguard): In terms of utilizing u-health medical equipment, how to address responsibility concerns resulting from unauthorized remodeling of equipment or the use of unverified update methods, or the like must be clarified in corresponding documents. Where the responsibility lies must be clarified in preparation for the occurrence of security issues among users, equipment manufacturers and sellers.
1004	(Mandatory) Countermeasures against security breaches (administrative safeguard): A communication channel that can be used for connecting emergency contacts and consulting equipment manufacturers must be provided with regard to security breaches that may occur while using u-health medical equipment, at the same time establishing counter policies against critical security breaches.
1005	(Mandatory) Voice feedback selection functions (technical safeguard): Voice feedback is being recommended as a very useful element for the visually impaired. However, the use of such devices in public places may result in the risk of leaking personal information. For this reason, (1) the functions that may expose personal information must be excluded from voice feedback functions, or (2) a function that can disable voice feedback, or (3) a function that allows users to utilize earphones or the like for voice feedback is required. This item only applies to u-health medical equipment with voice feedback functions
1006	(Mandatory) Limitations on displaying personal health information (technical safeguard): In u-health, there is no way of knowing the environments to which users are currently exposed. Therefore, no personal health information should be displayed unless otherwise requested by users.
1007	(Mandatory) Guaranteeing the integrity of firmware and software updates (technical safeguard): The integrity of firmware and software updates must be guaranteed.
1008	(Mandatory) Approval of firmware and software updates (technical safeguard): There should be some processes that can be used for requesting and checking user requests for firmware and software updates. In terms of applying firmware and software updates, it is important to apply such updates after completing approval processes via pop-up windows, etc.
101	Common security elements for u-health measuring equipment
1011	(Mandatory) Emergency access functions (technical safeguard): U-health medical equipment is designed for using in conjunction with networks. However, it is recommended to include emergency access functions so that u-health medical equipment can be used in emergencies in specific circumstances. This item only applies to u-health medical equipment with built-in information display functions, and small-sized devices free from built-in information display functions are excluded from this category.
102	Common u-health gateway security factors

1021	(Mandatory) Recognition of the access of u-health measuring equipment (technical safeguard): The access of any device other than u-health measuring equipment approved by the gateway must be recognized and discerned.
1021	(Recommended) Access control of u-health measuring equipment (technical safeguard): A u-health-only gateway should be used whenever possible and if the gateway is also used as a general network gateway, a function that can discern networks types and processes accordingly is required. Though the access control of u-health measuring equipment by a gateway is deemed to be a very critical security factor, actual implementation of access control is quite tricky due to the updates and connection types of u-health measuring equipment. For this reason, this item is specified as "recommended."
103	Common security factors for support software
1031	(Mandatory) Integrity of support software (technical safeguard): It is required that support software must be equipped with self-inspection functions that can check whether the software is affected by malicious code or the system errors during the start-up.
1032	(Mandatory) Date integrity (technical safeguard): It is required that support software should be equipped with a self-inspection function which can check whether data, such as the saved personal health information or DSSH rules (if applicable), is affected by malicious code or the system errors.
1033	(Mandatory) Data encryption (technical safeguard): All data including user information must be encrypted at appropriate levels prior to being saved. A level of encryption that cannot be read by text readers or editors must be applied to user data, even if the included information is trivial.
1034	(Mandatory) Data backup for mobile media (technical safeguard): Data backup using mobile media, such as USB drives or the like, is prone to leaking personal health information as a result of loss or theft. Therefore, backup with low mobility media, such as CD ROMs, or the like, may be a better alternative for security reasons.
1035	(Mandatory) Data recovery functions (technical safeguard): Data recovery functions based on encrypted backup, etc., can be added in preparation for unexpected loss of personal health information. It is recommended that u-health servers, the security of which is certified, should be used for storing personal health information in a u-health system. For individuals, the risk of data loss is very high due to PC hard disk failures, etc. For this reason, if data is stored in PCs or smart phones, the users may selectively use such data recovery functions.
110	Common security factors by hardware portability
1101	(Mandatory) Use of disassembly-prevention seals (technical safeguard): Disassembly-prevention seals can be applied to u-health medical equipment. Users can check whether their equipment has been disassembled before by checking the integrity of the disassembly-prevention seals, and in doing so, the possible information leaks regarding personal health information can be checked. Disassembly-prevention seals must be attached to appropriate positions.
1102	(Mandatory) Warning signs for disassembly-prevention seals (administrative safeguard): It is required to attach disassembly-prevention seals to u-health medical devices. Users can check whether the equipment has been disassembled before by

	inspecting the integrity of the disassembly-prevention seals, and in doing so, the risk of information leakage regarding personal health information can be checked. Users should be aware of what kind of legal responsibility follows the malfunction of equipment after removing the seals for unauthorized repair work. In particular, the detachment of disassembly-prevention seals may put the equipment at the risk of a security breach in terms of personal health information, and the precaution clarifying that users shall be held accountable for the consequences of such action must be attached to packing boxes or be included in the user manuals.
1103	(Recommended) Secure display (physical safeguard): It is recommended that viewing angles should be reduced using secure displays such as security films in order to prevent the leakage of personal information from u-health medical equipment.
111	Non-portable items: Non-portable items refer to the items that are more than 5 kg in weight or more than 500 cm^3 in volume.
1111	(Mandatory) Providing fixation structures for equipment (physical safeguard): For non-portable u-health medical equipment, such equipment is exposed to high risk of being used by many different individuals, and needs to be fixated at table or wall surfaces in order to prevent theft. For this reason, physical fixation structures, such as fixation-purpose shallow screw holes, or the like, should be provided.
1112	(Mandatory) Descriptions on how to fixate equipment (administrative safeguard): For non-portable u-health medical equipment, such equipment is exposed to a high risk of being used by many different individuals, and needs to be fixated at table or wall surfaces in order to prevent theft. For this reason, physical fixation structures, such as fixation-purpose shallow screw holes, or the like. User manuals or their equivalents must include how to fixate the equipment.
1113	(Mandatory) Physical disassembly prevention of non-portable u-health medical equipment (physical safeguard): In many cases, the internal parts of u-health medical equipment are the targets of theft. Therefore, non-portable medical equipment must be designed in such a way that the internal parts of the equipment cannot be checked without using appropriate tools, and disassembly work must require a certain period of time. Non-portable u-health medical equipment must be designed in such a way as to require one to spend more than 10 seconds when checking key internal parts using electric drivers.
112	Portable items: Portable items refer to the items that are less than 5 kg in weight and less than 500 cm^3 in volume.
1121	(Mandatory) Physical disassembly prevention of u-health medical equipment (physical safeguard): Though it may sound contradictory, in many cases, the internal parts of u-health medical equipment are the targets of theft. Therefore, non-portable medical equipment should be designed in such a way that the internal parts of the equipment are not checkable without using appropriate tools. Design levels that prevent portable u-health medical equipment from being disassembled by hand should be applied.
1122	(Recommended) Application of UDIs (unique device identifiers) (technical safeguard): Portable u-health medical equipment is always exposed to a risk of theft. If this is the case, the use of UDIs or similar technologies is recommended in order to trace the location of lost equipment. The full-fledged UDI technology is under a standardization process, and the mandatory application of UDIs by law may

	not be realized in the short term, hence the limitations on UDIs or similar technologies. Here, similar technologies mean a set of technologies capable of identifying serial numbers allocated to manufactured medical equipment in u-health service systems.
12	U-health medical equipment: Security factors related to personal identification
120	Common security factor on personal identification: RESERVED
121	Devices free from personal identification functions: The devices free of personal identification functions or the devices the personal identification functions of which are performed by smart phones or PCs or gateway software, such as small-sized blood sugar testing dongles, etc.
1211	(Mandatory) Gateways without personal identification functions are not allowed (administrative safeguard): Personal identification functions are required for configuring gateways.
1212	Devices with personal identification functions: Here, personal identification functions are largely broken down to three types, and overlapped selection is also possible. The three types are as follows: (1) Personal identification through user inputs, such as IDs, passwords, PINs, etc.; (2) automatic identification through biometric recognition functions that do not require such operations; (3) Personal identification through personal recognition media, such as RFID cards, USB drives including official certificates, magnetic cards, etc.
1220	Common security factors
12201	(Mandatory) An automatic session timeout must be enabled after a certain period of time unless u-health medical equipment remains active after log-in (technical safeguard). A session timeout shall not exceed a maximum of 5 minutes.
1221	Personal identification media: All types of media used for identifying individuals, such as USB drives including official certificates, magnetic cards, etc.
12211	(Mandatory) Log-in to personal identification media (administrative safeguard): For "signing in" through personal identification media, personal identification functions based on PINs or biometry must be included.
12212	(Recommended) Session timeout in personal identification media (technical safeguard): For signing in using personal identification media, the use of additional session timeout functions for a certain period of time, as is the case with general session timeout functions, is recommended.
1222	PIN-based log-in methods: general log-in methods
12221	(Mandatory) Overlapping of user IDs (technical safeguard): User IDs must be assigned without being overlapped.
12222	(Mandatory) Encryption of passwords (technical safeguard): All passwords must be saved as hash values that are not replicable in the event of information leakage. Encryption methods can be divided into two types: one is two-way decryption which allows one to find original texts used as passwords by decrypting the encrypted passwords, and the other is one-way encryption. The one-way encryption helps to increase security levels because even administrators are not able to identify passwords.
12223	(Mandatory) Exposure of passwords (technical safeguard): All passwords should be expressed as "***" in displays during entry in order to prevent them from being

	exposed to others.
1223	Biometric identification: Personal identification based on biometric information, such as fingerprints, irises, faces, and the like, or combinations of biometric information
12231	(Mandatory) Encryption of biometric identification templates (technical safeguards): All biometric identification information must be encrypted upon entry at biometric sensor terminals.
12232	(Mandatory) Copy protection of biometric information templates (technical safeguard): All encrypted biometric information templates shall not be replicable. The key of biometric information security is to store templates only as hash data without leaving the templates behind.
12233	(Recommended) Verification of live biometric identification information (technical safeguard): Biometric identification information may easily be faked depending on technical applications. As information regarding the identification of faces or fingerprints or the like may be leaked using photos or the like, the use of a function which can verify live biometric information is recommended.
12234	(For reference) 3D facial recognition (technical safeguard): Facial recognition using a 3D stereo camera may reduce the risk of a security breach that may occur by faked biometric information, using ordinary photos.
13	U-health medical equipment: Transmission-related security factors
130	Common items for transmission-related security factors
1301	(Mandatory) Displaying connection status (technical safeguard): The connection status of users should be displayed when the users are connected to storage devices, gateways or other networks, etc.
1302	(Mandatory) Displaying transmission status (technical safeguard): There should be no case in which personal medical information is transmitted for malicious purposes without being noticed by users. Therefore, the transmission of information from u-health medical equipment must be displayed as blinking LEDs or on screens or the like so that users can monitor whether information is being transmitted when independently being connected to other networks.
131	Measuring devices designed to be connected with mobile phones or PCs or the like via USD cables, and the like, without built-in networking functions.
1311	(Mandatory) The use of gateways without networking functions is prohibited (administrative safeguard): There exists no gateway that lacks networking capabilities.
1312	(Mandatory) Use of standard transmission protocols (technical safeguard): Data transmission must be performed using standard hardware or software technologies, such as USB, IEEE 1394, etc. As such standards had been established in consideration of security features, such as basic integrity levels, at the same time guaranteeing compatibility, it is important to use standard transmission protocols.
132	Network support
1320	Common security factors for network support
13201	(For reference) Remote data destruction (technical safeguard): Functions allowing users to destroy critical personal medical information by remote may be added. At this point, a high level of security technology is additionally needed for the

	transmission of target code. Remote data destruction has emerged as one of the most important technologies on the Internet in recent days.
1321	Closed network support
13211	(Mandatory) Encryption of personal health data over closed networks (technical safeguard) Encryption must be applied. For closed networks, the risk of information leakage is relatively low in communications channels. Though closed networks do not require VPN-like technologies, a minimum level of encryption should be applied.
1322	Open network support
13221	(Mandatory) All personal health data shared via open networks must be encrypted through VPN encryption techniques, such as SSL, IPSec, etc.
14	U-health medical equipment: Security factors related to handling individual health data
140	Common security factors related to handling individual health data: RESERVED
141	Unsaved individual health data: Small-sized dongle-like measuring devices designed to be connected with handsets, etc. : RESERVED
142	Storing a small amount (less than 10 persons) of individual health data: Storing personal information, such as user IDs, passwords, etc.
1421	(Mandatory) Limitations on the range of personal information that can be collected (administrative safeguard): Collecting unnecessary personal information is not allowed. It should be noted that this is a prerequisite in terms of general personal information protection.
1422	(Mandatory) How to store personal information (administrative safeguard): How to save individual health data from technical perspectives must be described in user manuals in order to help users to understand critical security features.
1423	(Mandatory) Destruction of personal information (administrative safeguard/technical safeguard): How to delete personal information must be clarified in user manuals, allowing users to destroy saved personal information on their own, if necessary. For users wanting to destroy personal information, their personal information must be deleted once and for all at appropriate levels. The appropriate levels refer to levels at which simple data recovery in the FAT format is impossible.
143	Storing a large amount (more than 10 persons) of personal information: Personal information, such as user IDs and passwords, is retained (RESERVED). Much more enhanced security standards must be applied when storing a large amount of personal data, compared with storing a small amount of individual health data. However, as there is no strong need for distinguishing the two at the current level, a large amount of data should be retained as "RESERVED," and the items applied to the storage of a small amount of individual health data must be applied to the storage of a large amount of data in the same way.
15	Security factors related to u-health medical equipment support software: This support software should be applied to the software provided by u-health medical equipment manufacturers, along with the main bodies of medical equipment. However, this software is not applied to some u-health systems with software running in system operation layers, such as active-X, connection programs, etc.

150	Common security factors regarding support software
1501	(Mandatory) Session timeout (technical safeguard): All sessions must be timed out after a certain period of time after log-ins. The maximum session timeout shall not exceed five minutes (2010, the Ministry of Health and Welfare) [20].
1502	(Mandatory) The data used by all support software must be encrypted prior to being saved. The encrypted data shall not be identifiable using ordinary text editors or binary editors.
1503	(Mandatory) Integrity self-check functions (technical safeguard): Some functions capable of verifying the integrity of the files of support software and linked data files must be provided.
1504	(Recommended) Keystroke capture prevention technology (technical safeguard): The application of keystroke capture prevention technology is recommended in order to prevent information leakage.
1505	(For reference) It is recommended that individual health data should not be saved on clients (technical safeguard): Given the purposes of u-health services, not saving individual health data on client hardware is advantageous in terms of increasing security. Saving individual health data on ordinary PCs increases the risk of leaking individual health data even if the data is encrypted. For this reason, not saving individual health data on clients can be a better alternative for security reasons. Therefore, such recommendations should be provided in the form of pop-up windows. In addition, allowing users to select not saving individual health data on clients as a default option on client software can be a good way to increase security.
151	There is no device support function: RESERVED
152	There is a device support function
1521	(Mandatory) Device diagnosis functions (technical safeguard): Functions allowing users to check for the presence of any malfunction of their devices using the data obtained from the devices are required. Whether or not a device functions normally can be inspected by checking the operation of the device using the data obtained from a measuring device or the firmware, etc.

3. Considerations and Conclusions

A variety of information security standards, guidelines, related statutes, certification programs, and the like have been analyzed in this study, at the same time suggesting new assessment items and methods that had been collected and developed after extracting security requirements that can be applicable to the real-world situations in u-health environments. In addition, the factors that might be the sine qua nons of more rigorous personal medical information protection schemes in the future are also included and described as recommendations. The individual assessment items for u-health medical equipment, which has been prepared over the course of such research processes, may help increase security levels in terms of the design of u-health medical equipment. However, the u-health market still remains its infancy, with more issues that need to be materialized in connection with the legal identity of u-health. For this reason, despite the effort made to define the maximally sustainable security items for u-health medical devices after collecting the opinions of the experts involved in the u-health

medical equipment industry during the course of conducting this research, a number of uncertainties still remain in some items due to the lack of verification processes in the actual u-health market, given their standards and requirement levels. Ultimately, it is believed that more sustainable studies should be carried out in line with the ontogeny of the u-health market.

Acknowledgements

1. This study is the result of the u-health project(10172 u-health 461) supported by the Korea Food and Drug Administration(KFDA).

2. This research was financially supported by the Ministry of Education, Science Technology (MEST) and National Research Foundation of Korea (NRF) through the Human Resource Training Project for Regional Innovation.

References

[1] Ministry of Health and Welfare, "2009 National Health Statistics", administrative publication no. 11-1351159-000027-10, Korea, **(2010)**.
[2] Ministry of Health and Welfare, "2010~2020 Long term estimation for national health expenditure", Korea **(2011)**.
[3] Samsung Economic Research Institute, "A new era of u-Health", Korea **(2007)**.
[4] ISO/IEC 27001: 2005 Information technology - Security techniques - Information security management systems - Requirements, Switzerland, **(2005)**.
[5] ISO/IEC 27002: 2005 Information technology - Security techniques - Code of practice for information security management, Switzerland, **(2005)**.
[6] ISO 27799: 2008 Health informatics - Information security management in health using ISO/IEC 27002, Switzerland, **(2008)**.
[7] IEC 60601-1-4: 2000 Ed 1.1b Medical electrical equipment - Part 1-4: General requirements for safety - Collateral standard: Programmable electrical medical systems, USA, **(2000)**.
[8] IEC 60601-1-11: 2010 Ed 1.0b Medical electrical equipment - Part 1-11: General requirements for basic safety and essential performance - Collateral Standard: Requirements for medical electrical equipment and medical electrical systems used in the home healthcare environment, USA, **(2010)**.
[9] HIPAA 45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule, USA, **(2006)**.
[10] HIPAA 45 CFR Parts 160 and 164 Standards for Privacy of Individually Identifiable Health Information; Final Rule, USA, **(2006)**.
[11] Ministry of Public Administration and Security, Personal information protection law, no. 10465, Korea.
[12] Korea Communications Commission, Information communication network use promotion and information protection law, no. 10560, Korea.
[13] Ministry of Health and Welfare, Medical law, no. 11005, Korea.
[14] Korea Communications Commission, "Technical and administrative protection action criteria of personal information", (Notification No. 2011-01 of the Korea Communications Commission), Korea, **(2011)**.
[15] Korea Food and Drug Administration, "u-Healthcare itemwise medical device permission and evaluation guideline", Korea, **(2010)**.
[16] Telecommunications Technology Association, "Technical requirements for personal health information protection", TTAK.KO-10.0304, Korea, **(2008)**.
[17] Telecommunications Technology Association, "Tele-bio identification protection procedure - Technical and administrative guideline for bioinformation protection", TTAK.KO-12.0034/R1, Korea, **(2009)**.
[18] Korea Information Security Agency, "Fulfillment guidebook for personal information impact assessment of public institution", (revised edition), no. 11-1311000-000221-01, Korea, **(2011)**.
[19] Ministry of Health and Welfare, "Personal information protection guideline of a medical institution", Korea, **(2010)**.