Abstract

The present study analyzed the current state and related issues of standardization of personal medical information security by probing information security standards, guidelines, related statutes and certification programs in order for Korea to take initiatives in international standardization of security for ubiquitous healthcare (u-health). We chose essential elements of privacy, security and safety to investigate the international standardization status; in user privacy, user authentication, user ID security, and user identification, in health information security, data security, security infrastructure, accountability assurance, communication security, ID management and access control, non-repudiation, security management, and backup, storage, archiving, disposal, in safety, risk management, technology for emergency access, disassemble prevention and fixation, and equipment error check. As a result, we came up with the conclusion that Korea must immediately take the initiative of developing an international standard that addresses the overall safety of medical equipment, including emergency access, electrical malfunctioning management, and operational condition check.

Keywords: Personal Medical Information, Privacy, Security, Safety, Standardization, Ubiquitous Healthcare

1. Introduction

Ubiquitous healthcare (U-health) is an emerging technology that employs large of patient sensors to monitor the condition of patients. However, many patients are concerned about the privacy and security of personal medical information that is used in this technology. The confidentiality and integrity of personal medical information must be maintained while making it available to trusted healthcare professionals.

Today, medical technology professionals are trying to develop uniform standards that can be applied throughout the world. A standard not only helps in regulation of products but also paves the way for a specific company that tries to introduce and distribute such products in global markets. This is achieved by eliminating unnecessary technical trade barriers, such as the use of different standards in different countries. In other words, the reach of a product in different markets is enhanced by designing compatibility assessment systems. Even official international organizations have emphasized on the application of uniform standards in global markets. For example, the Technical Barriers to Trade (TBT) is an agreement that is administered by the World Trade Organization (WTO). According to this agreement, when a member country revises an existing standard or establishes a new national standard, it must take into consideration the existing international standards.

In this context, the International Standard Organization (ISO) has compiled an international standard that incorporates the principles of local standards on medical information security. The objective of international standardization is to minimize risk and maximize mutual benefit by bringing about consensus between different companies. As a result, only those companies that participate in international standardization would be able survive in the future. In u-health technology, Electronic Medical
Records (EMR) and Personal Health Records (PHR) are interconnected; therefore, the standardization of medical information security is required for maintaining the privacy and integrity of medical information during the various stages of acquisition, transmission and storage.

It is difficult to acknowledge that the international and domestic standards optimized for the medical center and ISO 27799 merely define the best practice of ISO 27002. Therefore, Information Security Management System (ISMS) standard needs to be developed to cover major issues, such as outpatient, hospitalization, and emergency: the actual components of a system’s medical process.\(^4,5\)

Although many methods have suggested text mining and rule-based system, the development ISMS standard is still in its early stage.\(^6\) In this study, a variety of information security standards, guidelines, related statutes, and certification programs have been analyzed to extract security elements for Korean candidates. Thus, we have taken initiatives in developing international standardization related to u-health environments.

### 2. Materials and Methods

We analyzed standardized items for technical classification and institutionalization Table 1. By analyzing related technologies, we created a map of related technology and standard, and then we chose items to be standardized as per Korean initiative Table 2.

<table>
<thead>
<tr>
<th>Related technology</th>
<th>Standardization institute/group</th>
<th>Standardization status</th>
<th>Technology status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Korea</td>
<td>overseas</td>
<td>Korea</td>
</tr>
<tr>
<td>User authentication</td>
<td>TTA KATS</td>
<td>ISO/IEC</td>
<td>-</td>
</tr>
<tr>
<td>ID security</td>
<td>TTA, KATS</td>
<td>ISO</td>
<td>-</td>
</tr>
<tr>
<td>User identification</td>
<td>TTA KATS</td>
<td>ISO/IEC JTC1</td>
<td>instituted</td>
</tr>
<tr>
<td>Data security</td>
<td>TTA KATS</td>
<td>ISO/IEC JTC1</td>
<td>instituted</td>
</tr>
<tr>
<td>Security infrastructure</td>
<td>TTA KATS</td>
<td>ISO/IEC</td>
<td>-</td>
</tr>
<tr>
<td>Accountability</td>
<td>TTA KATS</td>
<td>ISO</td>
<td>instituted</td>
</tr>
<tr>
<td>Communication (messaging) security</td>
<td>TTA KATS</td>
<td>ISO/IEC HL7</td>
<td>instituted</td>
</tr>
<tr>
<td>ID management/access control</td>
<td>TTA KATS</td>
<td>ISO ASTM</td>
<td>Partially instituted</td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>TTA KATS</td>
<td>ISO/IEC HL7</td>
<td>instituted</td>
</tr>
<tr>
<td>Security management</td>
<td>KATS</td>
<td>ISO ASTM</td>
<td>-</td>
</tr>
<tr>
<td>Security policy</td>
<td>KATS</td>
<td>ISO ASTM</td>
<td>-</td>
</tr>
<tr>
<td>Safe backup/storage/archiving/disposal</td>
<td>TTA KATS</td>
<td>ISO</td>
<td>instituted</td>
</tr>
<tr>
<td>Risk management</td>
<td>TTA KATS</td>
<td>ISO/IEC</td>
<td>instituted</td>
</tr>
<tr>
<td>Emergency access</td>
<td>TTA KATS</td>
<td>ISO/IEC</td>
<td>-</td>
</tr>
<tr>
<td>Disassemble prevention</td>
<td>TTA KATS</td>
<td>ISO/IEC</td>
<td>-</td>
</tr>
<tr>
<td>How to fix</td>
<td>TTA KATS</td>
<td>ISO/IEC</td>
<td>-</td>
</tr>
<tr>
<td>Equipment error check</td>
<td>TTA KATS</td>
<td>ISO/IEC</td>
<td>-</td>
</tr>
</tbody>
</table>
Table 2. The map of related technologies and elements to be standardized in Korea

<table>
<thead>
<tr>
<th>Classification</th>
<th>Definition</th>
<th>Elements to be standardized</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy protection technology</td>
<td>User authentication technology</td>
<td>User authentication technology</td>
</tr>
<tr>
<td></td>
<td>ID security technology</td>
<td>Pseudonymisation and anonymisation technology</td>
</tr>
<tr>
<td></td>
<td>User identification technology</td>
<td>Code-based user identification technology</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RFID/IC card-based user identification technology</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PIN-based user identification technology</td>
</tr>
<tr>
<td>Health information security technology</td>
<td>Data security technology</td>
<td>Confidentiality assurance technology</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Integrity assurance technology</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Availability assurance technology</td>
</tr>
<tr>
<td></td>
<td>Security infrastructure</td>
<td>PKI technology</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Directory service technology</td>
</tr>
<tr>
<td></td>
<td>Accountability technology</td>
<td>Audit trail technology</td>
</tr>
<tr>
<td></td>
<td>Communication (messaging) security technology</td>
<td>VPN technology</td>
</tr>
<tr>
<td></td>
<td>ID management/access control technology</td>
<td>Intrusion detection and prevention technology</td>
</tr>
<tr>
<td></td>
<td>Non-repudiation technology</td>
<td>Non-repudiation technology</td>
</tr>
<tr>
<td></td>
<td>Security Management technology</td>
<td>Information security management system technology</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Technology for reserving/registering/hospitalization/discharge from hospital/transfer/amendments</td>
</tr>
<tr>
<td></td>
<td>Security policy</td>
<td>Security policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Health management authentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security training</td>
</tr>
<tr>
<td></td>
<td>Safe backup/storage/archiving/disposal technology</td>
<td>Safe backup/storage/archiving/disposal technology</td>
</tr>
<tr>
<td>Medical equipment safety assurance technology</td>
<td>Risk management technology</td>
<td>Risk management technology</td>
</tr>
<tr>
<td></td>
<td>Emergency access technology</td>
<td>Emergency access technology</td>
</tr>
<tr>
<td></td>
<td>Disassemble prevention technology</td>
<td>Disassemble prevention technology</td>
</tr>
<tr>
<td></td>
<td>How to fix</td>
<td>Fixing method</td>
</tr>
<tr>
<td></td>
<td>Equipment error check technology</td>
<td>Equipment abnormality check technology</td>
</tr>
</tbody>
</table>

3. Results

Current status and issues of focusing technology

3.1 User Privacy

3.1.1 User Authentication Technology

- The US Federal Health Insurance Portability and Accountability Act (HIPAA) Security Rule §164.308 is an administrative safeguard that stipulates the authentication of employees through information access management, such as access policies, procedures, and access authorization of a medical information center; it is a guiding document from the National Institute of Standards and Technology (NIST).7
- Canada is developing a guideline under the leadership of the Canada Health Infoway (CHI). Furthermore, CHI SCWG8 IT Privacy and Security Services are conducting a standardization research.8
ISO/TC 215, which takes initiatives to establish International Health Informatics Standard, is not working on a specialized standardization that could be used in authenticating a medical information system. However, the ISO published a standard on the electronic signature technology or authentication technology, which uses an encoding algorithm or hash algorithm for authenticating general information system.

Europe has also been developing a standard that focuses on electronic signature, which is one of the authentication tools.

Korea has taken initiatives on developing a standard that focuses on electronic signature, which is one of the authentication tools.

The medical information system is such that there is not a significant difference in the mechanism of different security technologies, such as digital signature, time stamp and encoding algorithm. Nevertheless, we need to standardize the ways of authenticating each of those technologies involved in the medical information system.

3.1.2 User ID Security Technology - Pseudonymisation and Anonymisation

The US is working on anonymisation in accordance with the Safe Harbor Framework that proposes to delete all 18 Personal Health Information Identifiers described in the HIPAA.

Safe Harbor Framework focuses on only deleting the direct identifier, while individual researchers are working on a quasi identifier.

The studies on genetic information have become extensive in recent times. Therefore, researchers have started investigating the security of user ID; user ID of patients is imperative in gaining access to their genetic and medical information.

Canada has developed and proposed the guidelines for the security of user ID based on the initiatives of CHI.

The deletion of a direct personal identification code like the social security number has been standardized.

With the help of current technology, it is not easy to delete the personal information that is recorded in the text format on a medical chart. Nevertheless, researchers have proposed many methods that are based on the text mining and rule-based system. However, these methods are still in the early stages of development.

Although researchers have been successful in developing novel technology to delete the quasi identifier, very few research studies have focused on this technology. Data modification can damage the accuracy of medical data, so this technology is not appropriate in its nature. Therefore, several studies only focus on data suppression. In this case, an honest broker is used to maintain k-anonymity and pseudonymisation.

3.1.3 User Identification Technology

The user identification and authentication technology efficiently maintains a secure system.

Most medical systems identify the user by checking the validity of code or Personal Identification Number (PIN), which is based on knowledge-based technology.

The Integrated Circuit (IC) card is issued to visiting patients; it is as an offline electronic card and can be used for the following purposes: identification, authentication, reception, prescription, treatment information, and access control. Thus, many hospitals in Korea and overseas have introduced it.

Radio-Frequency Identification (RFID) technology is used to identify patients and manage medicines, medical equipment, and infectious wastes.

We do not have a separate standard to identify and authenticate the users. However, many standards deal with it partially.

3.2 Health Information Security

3.2.1 Data Security Technology that Ensures Confidentiality, Integrity and Availability

Data security technology has been studied extensively in many research studies. Moreover, many products based on this technology have introduced in the market. However, many specific technologies have their own standard.

3.2.2 Security Infrastructure – Public Key Infrastructure (PKI) Technology, Directory Technology

Public Key Infrastructure (PKI) technology is not at all new as government agencies have been using it since many years. Presently, it has been developed for
commercial use. However, the international standard on PKI was instituted along with the ISO to ensure that hospitals and health centers protect medical information. Nonetheless, it does not correspond with the Korean standard. Therefore, it is must be developed to comply with the Korean standard; then, we can develop innovative technology accordingly and apply it to hospitals and healthcare centers.

3.2.3 Accountability Assurance Technology - Audit Trail Technology and Log Management Technology

- After the ISO created an international standard, a new standard was developed in Korea last December to comply with the international standard. It is expected that hospitals and related companies would develop and apply it from this year.

3.2.4 Communication Security Technology: Virtual Private Network (VPN), Intrusion Detection and Prevention Technology

- In the traditional security paradigm, the standard on communication security was already instituted by the ISO IEC. The ISO along with others is establishing a standard for medical information accessed through dynamic VPN. Thus, this standard would define health information infrastructure and security standard for Electronic Health Record (EHR) communication. Messaging security for transmission has been recently released as Health Level 7 (HL7) Version 3.0.
- Meanwhile, Korea and Europe made HL7 Version 3.0 to comply with their own standards. In this case, the hospitals, businesses, and academic circle in Korea will have to practically develop and apply the standard.

3.2.5 ID Management and Access Control Technology

- It comprises of integrated authentication and authority management technology, which enables efficient management of access control to the entire medical system, such as EMR, Order Communicating System (OCS) and Hospital Information System (HIS).
- As exchange of medical information is necessary, research studies are defining access policy of hospitals by investigating the management of user ID from both inside and outside the hospitals.

- Furthermore, researchers are actively developing an access control technology that is based on appropriate medical information systems that consider various access environments, such as the mobile environment.
- The service that is provided uses Federation-ID and is based on Security Assertion Markup Language 2.0 (SAML 2.0).
- Functional-structural sets and models are defined so that the access can be controlled, depending on the user role for the ISO/TC215 WG4 pseudonymisation task group.
- In particular, the medical application service model is more focused on defining the role of the patient and medical service personnel. It considers that each model can be classified into structural (static) or functional (dynamic) types.

3.2.6 Non-Repudiation Technology

- Non-repudiation is applied to a message sent and received within HL7 Version 3.0. Therefore, it is anticipated that hospitals and related institutions would practically develop and apply it henceforth.

3.2.7 Security Management

- Information Security Management System (ISMS) certification is an external objective evaluation tool that is used to judge ISMS of an organization. Korea Internet and Security Agency (KISA) implements the ISMS standard in Korea. It is associated with ISO27001.
- The US uses the federal HIPAA Security Rule that comprehensively describes each information security management system ($164.308, $164.310, $164.312$).
- American Society for Testing and Materials (ASTM) Standard defines the object-centered model for an information system that is used for processing the information of a medical center, such as patient registration and the people getting admitted or discharged from the hospital (ASTM E1715).
- Canada, which is developing the guideline under the leadership of CHI and CHI SCWG8 IT Privacy and Security Services, is conducting the study on the standardization.
- ISO TC 215, which has taken initiatives to establish International Health Informatics standard, announced the standard that integrated ISO27000 series into the medical sector (ISO 27799).
- Europe has also complied with BS7799 of the British Standards Institution (BSI) from 1995.
However, it is difficult to ensure that the international and domestic standards are optimized for the medical center, because ISO 27799 merely defines the best practice of ISO 27002. Therefore, ISMS standard needs to be developed to cover major issues, such as outpatient, hospitalization, and emergency: key components of the medical system.

3.2.8 Security Policy: Security Policy, Health Management Certification, Security Training

- The UK wrote and distributed for the first time the BS7799-1, which is an information security management standard. This standard also has ISO/IEC 17799 based on it. Furthermore, this standard was published before introducing BS7799-2 certification system, which is based on it. The certification system was accepted by EA and implemented.
- ISO/IEC 17799 Code of Practice for Information Security Management is the international standard for information security management; the control items for information security were segmented and increased as BS7799 was changed to ISO27001.
- KISA in Korea also runs personal information management system certification by categorizing this certification into ISMS, Personal Information Management System (PIMS), and Government Information Security Management System (G-ISMS).

3.2.9 Backup, Storage, Archiving, Disposal

- The Korean standard for this area was made to conform with that of the ISO. Accordingly, we anticipate that the hospitals and related companies can practically develop and apply it as soon as possible.

3.3 Safety

3.3.1 Risk Management Technology

- Risk management standard on medical software is primarily standardized internationally along with the ISO. In 2010, the Ministry of Food and Drug Safety (MFDS) of Korea also successfully ensured that its standard complies with the international one for risk classification and patient safety.
- However, it is necessary to immediately introduce the risk management standard on medical equipment.

3.3.2 Technology for Emergency Access, Disassembly, Prevention and Fixation

- MFDS along with others institutions compiled the requirements and guidelines for equipment evaluation in 2010. Yet, this standard has neither been prepared in Korea nor in other countries of the world.

3.3.3 Equipment Error Check - Equipment Abnormality Check Technology

- MFDS along with others institutions compiled the requirements and guidelines for equipment evaluation in 2010. Meanwhile, the ISO made recommendations for standardization that would define how a medical center would manage medical equipment and electronic malfunctioning while using wireless communication or computing technology.
- Therefore, an international standard under the leadership of Korea needs to be prepared urgently. This standard must address the overall safety of the medical equipment, including electrical malfunctioning management and operational condition check.

4. Discussion

The protection of privacy, security, and safety of personal health information is a must to provide a secure system. This would ensure good service in u-health environment. After discussing with many companies, authorities have devised international standardization, which is a process to minimize risk and maximize mutual benefit.

In this study, we investigated the current status and related issues of medical information security. Thus, we tried to understand the standardization strategy in Korea. After analyzing international and domestic information security standards, guidelines, related statutes, and certification programs, we chose some security elements of the following three aspects: user privacy, health information security, and safety. Finally, we concluded that Korea must take initiatives in international standardization for security issues associated with u-health environment. This is because the safety standards of medical equipment in Korea have not yet been defined as per international specifications.

Some international standards do not comply with the Korean standard. Therefore, it is necessary that Korea promotes domestic compliance of international standards through the Korean Agency for Technology and...
Standard (KATS)\(^{16}\) and Korea Standard Association\(^{16}\). This is because only those companies that participate in standardization would be able to do business in global markets in the near future. Therefore, it is necessary to make these companies compliant with the Korean standard. Thereafter, these companies would develop technology accordingly. Moreover, Korean standards must also be applied to hospitals and health centers.

Ultimately, it is believed that more sustainable studies should be carried out in accordance with the ontogeny of the u-health market. For example, in the US, as the studies on genes have become extensive recently, the study on the security of user ID was also conducted as this user ID converges the genetic and medical information of subjects\(^{17}\).

Conclusively, Korea must take initiatives in developing an international standard that defines the overall safety of medical equipment, including emergency access, electric malfunctioning management, and operational condition check.

5. Conclusion

Korea must take initiatives in developing an international standard that addresses the overall safety of personal medical information. This standard would ensure successful management of all kinds of information systems (including both hardware and software). Thus, Korea would be able to maintain its dominance in the global market.

6. Acknowledgment

This study is a part of the standard technology enhancement project, which is supported by Korea Standard Association (KSA).

7. References

8. Canada health infoway SCWG8. IT Privacy and Security Services; Canada. 2014.