Original Article

Healthc Inform Res. 2012 June;18(2):125-135.
http://dx.doi.org/10.4258/hir.2012.18.2.125
pISSN 2093-3681 • eISSN 2093-369X

HIR
Healthcare Informatics Research

Pitfalls and Security Measures for the Mobile EMR System in Medical Facilities

Kiho Yeo, BS[1], Keehyuck Lee, MD[1,2], Jong-Min Kim, MD, PhD[3], Tae-Hun Kim, MD[4], Yong-Hoon Choi, DDS, PhD student[5], Woo-Jin Jeong, MD, PhD[6], Hee Hwang, MD, PhD[1], Rong Min Baek, MD, PhD[7], Sooyoung Yoo, PhD[1]

[1]Center for Medical Informatics, Departments of [2]Family Medicine, [3]Neurology, [4]Thoracic and Cardiovascular Surgery, [5]Conservative Dentistry, [6]Otorhinolaryngology, and [7]Plastic and Reconstructive Surgery, Seoul National University Bundang Hospital, Seongnam, Korea

Objectives: The goal of this paper is to examine the security measures that should be reviewed by medical facilities that are trying to implement mobile Electronic Medical Record (EMR) systems designed for hospitals. **Methods:** The study of the security requirements for a mobile EMR system is divided into legal considerations and sectional security investigations. Legal considerations were examined with regard to remote medical services, patients' personal information and EMR, medical devices, the establishment of mobile systems, and mobile applications. For the 4 sectional security investigations, the mobile security level SL-3 from the Smartphone Security Standards of the National Intelligence Service (NIS) was used. **Results:** From a compliance perspective, legal considerations for various laws and guidelines of mobile EMR were executed according to the model of the legal considerations. To correspond to the SL-3, separation of DMZ and wireless network is needed. Mobile access servers must be located in only the smartphone DMZ. Furthermore, security measures like 24-hour security control, WIPS, VPN, MDM, and ISMS for each section are needed to establish a secure mobile EMR system. **Conclusions:** This paper suggested a direction for applying regulatory measures to strengthen the security of a mobile EMR system in accordance with the standard security requirements presented by the Smartphone Security Guideline of the NIS. A future study on the materialization of these suggestions after their application at actual medical facilities can be used as an illustrative case to determine the degree to which theory and reality correspond with one another.

Keywords: Mobile Electronic Medical Record, Mobile Picture Archiving and Communication System, Mobile Health Information System, Mobile Security, Smart Health Security

Submitted: May 18, 2012
Revised: June 5, 2012
Accepted: June 9, 2012

Corresponding Author
Sooyoung Yoo, PhD
Center for Medical Informatics, Seoul National University Bundang Hospital, 82 Gumi-ro, 173beon-gil, Bundang-gu, Seongnam 463-707, Korea. Tel: +82-31-787-1151, Fax: +82-31-787-4004, E-mail: yoosoo0@snu.ac.kr

I. Introduction

With the increased use of the wireless Internet and the expansion of the smartphone, the information environment has rapidly changed in recent years. As Internet usage transitions from a wired environment to a wired-and-wireless integrated environment, the market for various services and contents for mobile devices also grows [1]. Along with the expansion of mobile applications, many healthcare-related applications are being introduced [2]. In Korea, the concept which integrated medical services and information technology (IT) by using smart terminals, such as smartphones or tablet computer, spreads widely and invests in the mobile

health care area [3]. Hospitals are also active participants in this movement; many large hospitals or university hospitals that have already implemented an electronic medical record (EMR) system are trying to establish a mobile EMR system. A mobile EMR system that allows medical staff to access comprehensive information on a patient, including his or her medicine administration status, diet, vital signs, X-ray and computed tomography interpretations, and other basic information, through a mobile device has now become an irreversible trend.

Meanwhile, with the rapidly increasing use of mobile devices, the threats to mobile security have also continually grown. The need for discussions on the security of mobile devices that store essential information, including personal information, has been brought up recently and the prominence of discussions on the security of mobile devices is mentioned [1].

Smartphones, which combine computers and mobile telephones, are structurally vulnerable in terms of security; they display the security weaknesses of computers while also having a much higher potential for being hacked than ordinary cellular phones on a dedicated network [4]. Smartphones that use the Android-series operating system (OS) are more vulnerable to hacking because the OS's kernel functions can be modified for the following reasons: the public nature of the source; the ability to access the OS using multinetworks such as 3G, public Wi-Fi, private Wi-Fi, and Bluetooth; and the use of the online application store. As the phrase "PC on your palm" claims, smartphones support computer functionalities, which renders them vulnerable to malware [5-7]. In this environment, the appearance of a mobile EMR system that allows access to a patient's personal information and treatment history could be an ideal target for attackers.

This paper suggests which legal considerations and security requirements should be investigated. Additionally, this paper explores which security measures medical facilities must take when establishing a mobile EMR system that uses mobile devices.

II. Methods

This paper was based on the result of collaborative work with the working group of Korea Institute of Information Security & Cryptology. The security requirements for establishment of mobile EMR system were investigated and roughly classified into legal considerations and sectional security reviews by 3 security experts for 6 weeks. Legal considerations included the question of which authorities should be considered when establishing a mobile EMR system and the compliance of the system with the related laws, regulations, and guidelines issued by various agencies. In the sectional security reviews, the security level of mobile phones was first examined, and appropriate measures were proposed based on an examination of the ensuing security requirements that should be considered in the areas of smartphone terminal security, network security, server security, and administrative security.

1. Legal Considerations

Legal considerations should precede the review of a mobile EMR system's security requirements because legal considerations are crucial for executing the appropriate security measures and cost-effective security reinforcements as well as for preparing and complying with the policies of the various institutions that have authority over the medical facility.

Institutions that have enacted laws related to personal information protection and security at medical facilities include the National Intelligence Service (NIS) and the Ministry of Public Administration and Security (MOPAS). The Ministry of Health and Welfare, which handles the Medical Law, has enacted regulations that affect medical facilities as well. The Ministry of Education, Science, and Technology must also be mentioned in conjunction with public university hospitals. Other agencies that could affect medical facilities include the Korea Food and Drug Administration (KFDA), which affects picture archiving and communication system (PACS) and medical devices, and the Korea Internet and Security Agency (KISA), which plays a large role in various security-related areas. Figure 1 presents the laws, regulations, and guidelines of major institutions that must be reviewed by medical facilities when establishing a mobile EMR system.

In Figure 1, the rows show the related institutions, and the columns show the fields that must be investigated for each institution. This figure presents a model that includes all of the laws and regulations that must be investigated by medical facilities when establishing a mobile EMR system.

Based on this model, the legal review was conducted with respect to the following five considerations: 1) Legal considerations for remote medical services; 2) Legal considerations for patients' personal information and EMRs; 3) Legal considerations for medical devices; 4) Legal considerations for establishing a mobile system; and 5) Legal consideration for mobile applications.

During this legal investigation process, the NIS regulation of "Security standards for smartphones for business use by national and public institutions" (Security Standards) should be considered in relation to a mobile system. The regulation classifies mobile systems into four security levels based

http://dx.doi.org/10.4258/hir.2012.18.2.125

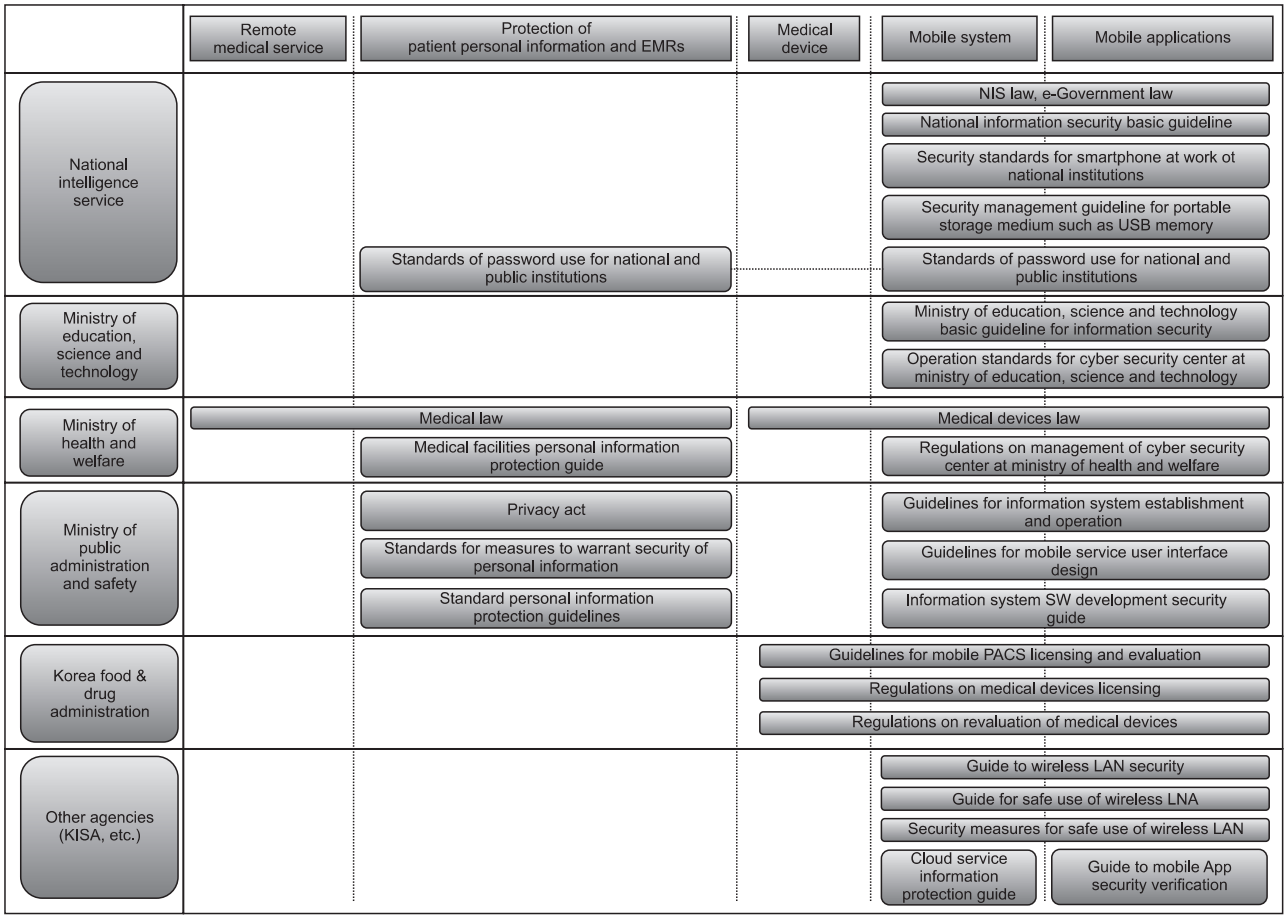

Figure 1. Model of the legal considerations to be reviewed by medical facilities.

on the work performed by the mobile system and describes the security requirements for each security level [8]. In particular, the regulation states that public university hospitals should strictly adhere to the Security Standards based on the "Ministry of Education, Science, and Technology Information Security Basic Guideline Article 55 (High Technology Telecommunications Device Security Administration)" [9]. Because the NIS's Security Standards are presented by an institution in charge of national security, they emphasize security reinforcement. Because Korean medical services are highly public and because the personal and medical information of all medical facilities' clientele should be protected, this paper conducted sectional security reviews based on these Security Standards.

2. Sectional Security Investigations

Prior to the sectional security reviews, the security level of a given institution in relation to the mobile system must be accurately understood. The aforementioned Security Standards classify the security level of a mobile system into the four levels. Furthermore, the security level systematically records common security threats to mobile systems and to the services conducted by each institution. The Security Standards that must be observed by an institution aiming to integrate smartphones into its business are also divided into levels.

The mobile security level differs based on the network structure of the institution and the importance level of the work data accessed by the smart terminal. Given the scope and composition of the mobile EMR system to be established, it is important to comprehend accurately the security level. Only after the security level is comprehended an institution can review the security requirements that match the security level and accurately apply the appropriate security measures [8].

The sectional security investigations subdivided security into the server, network, smart terminal and administration areas based on the Security Standards provided by the NIS for institutions that wish to implement smart terminals for business use. This study assumed that most medical facilities do not separate their networks and operate their internal medical information systems while using external mobile EMR systems. Thus, the mobile security level is set at SL-3. This paper investigated the security requirements set forth by the NIS for each section and suggested appropriate security measures to be taken in response.

III. Results

1. Legal Considerations

As mentioned previously, the legal considerations studied here focused on five aspects based on the model of legal considerations (Figure 1) that must be investigated by medical facilities when establishing a mobile EMR system.

1) Legal considerations for remote medical services

Because a mobile EMR system with remote medical services could create controversies (i.e., it provides an environment in which the medical staff can easily access a patient's information and treatment history at any time and place), the related laws were reviewed. Although only a few laws address medical information systems that use mobile devices, inferences can be made from the explicit statements on remote medical services in Article 34 of the Medical Law [10].

Clause 1 of Article 34 (remote medical services) of the Medical Law defines remote medical services as a medical provider's use of telecommunications technology to provide knowledge or technology to another medical provider located in a remote region. Thus, a mobile EMR system is not a remote medical service because it merely provides the means for a medical provider to access a patient's treatment history. However, in this case, the medical provider can only access the treatment history of his or her patients. Thus, if the medical staff can consult with the patient outside of the office and enter the information into the medical information system, the mobile EMR system must be examined from a different perspective.

2) Legal considerations for the personal information and EMRs of a patient

Allowing access to a patient's treatment history through a mobile EMR system means that only the people with justifiable grounds for accessing this information can do so. Other people are prohibited from accessing the information, as specified in Article 21 (access to records) and Article 23 (electronic medical record) of the Medical Law [10]. To comply with this stipulation, a mobile EMR system must verify the security of the people accessing the system. Additionally, an appropriate security measure must be taken if the mobile device is lost, as reflected in the measure for securing the safety of personal information that followed the implementation of the Personal Information Protection Law. The system should also comply with related notifications on access authority management, password management, personal information encryption, and security program operations corresponding to the contents of the Medical Facility Personal Information Protection Guideline announced in March 2010 by the Ministry of Health and Welfare [11,12]. For public medical institutions aiming to establish new mobile EMR systems, Privacy Impact Assessment must conform to the instructions on the Privacy Impact Assessment [13].

3) Legal considerations for medical devices

When establishing mobile PACS, medical institutions must examine the legal considerations for medical devices because PACS, a medical information system, is classified as a medical device and is licensed by the KFDA. Although the mobile device law makes no specific references to mobile PACS, with regard to the scope of the licensing examination, the KFDA's "mobile PACS licensing examination guideline" states that the "mobile PACS server and mobile PACS applications" constituting a mobile PACS system are the subject of licensing and examination under the medical device manufacturing and importing category of Articles 6 and 14 of the medical device law, respectively [14]. Furthermore, the KFDA should be notified if changes must be made to the mobile PACS software such that the software links with the mobile EMR system within a mobile EMR system.

4) Legal considerations for establishing a mobile system

Legal considerations for medical information systems that use mobile devices focus on the systems' compliance with technological security based on the Security Standards of the NIS. The security level set by the Security Standards must be understood, and the Security Standards compliance checklist in Phrase 2 of the Security Standards appendix must be checked to determine whether the guidelines for the given security level are being observed [8]. This topic will be examined more closely in the sectional security reviews. The technological security on a mobile system can be effectively strengthened by focusing on the parts of the system that do not comply with the Standards. Because it is difficult to find a law that suggests either public or private mobile system security standards with regard to these non-compliant parts, mobile systems should comply with the Standards in an identical manner.

Additionally, contents related to wireless local area network (LAN) security can be found in the "Security measures for safe use of wireless LAN" article published by the National Cyber Security Center or "Wireless LAN Security Guide" of the KISA [15,16]. Also available is the "Smartphone Security Guide" of the Financial Security Agency, which is in charge of security in the field of finance, where significant security reinforcement efforts were made following a recent chain of

http://dx.doi.org/10.4258/hir.2012.18.2.125

security breaches [17]. This guide describes the characteristics, security threats, and security considerations for each smartphone platform. Because this guide attempts to help prepare against security issues related to mobile services rather than the field of medicine, medical institutions should refer to this guide when establishing a mobile EMR system.

5) Legal considerations for mobile applications

The "Software Development Security Guide" published by the Ministry of Public Administration and Security in June 2011 is a regulation that should be examined in relation to mobile applications [18]. This guide compiles the different types of software security vulnerabilities and suggests a Secure Coding method for each language in which a mobile system is developed. Because applications with vulnerabilities removed during the development stage significantly reduce the expenses related to security measures, removing vulnerabilities is essential for improving the appeal of mobile applications. The fact that most of the recent cyber attacks involved the abuse of software security vulnerabilities should also be considered. For public medical institutions in particular, the request for proposals during the development contractor selection stage should clearly state that the contractor shall comply with Article 16 of Notification No. 2012-12 of the Ministry of Public Administration and Security, "Information System Establishment and Operation Guideline" [19]. Additionally, the contract and examination should show that the contractor complied with the "Software Development Security Guide" and executed "Security Vulnerabilities Inspections and Removals" according to Article 44 (software development security). Public medical institutions could utilize the certification service for mobile application security provided at no charge by the KISA. This service is well-documented in the Mobile Application Security Certification Guide published by the KISA in August 2011 [20].

2. Sectional Security Investigations

An institute interested in implementing a mobile EMR system should examine its own mobile security levels and review the ensuing security requirements before conducting the sectional security investigations.

1) Server security

Server security is designed to react to and prepare against intrusions that could occur within an internal system at a hospital. The server administrator is the agent in charge of all of the server's security requirements. The server security standards corresponding to the mobile security level SL-3 consist of administrator authentication, log management, and malware responses.

Administrator authentication should be further divided into account management and the timing of authentication. Furthermore, the authentication method and details should be investigated. In log management, the details of tasks should be documented with a focus on user activities, and a separate log server should be maintained. Malware responses begin by maintaining a host-based firewall to block unnecessary services and ports. The technological security measures that satisfy the server security requirements are shown in Table 1.

Server security should be coupled with measures for blocking and preventing intrusions. A firewall should be implemented and operated in the section linked with the telecommunications network to prevent hacking and unauthenticated connections to the mobile web server, and a system for detecting harmful traffic should be implemented and operated in the section linked with the telecommunications network to monitor abnormal traffic constantly.

Furthermore, a response system for threat management and intrusions should be implemented and operated for 24-hour security control. All of the servers should provide functionalities such as host-based firewall operations, password or authentication enforcement, log management, prevention of unnecessary ports, and access and authorities control. Public medical facilities could utilize the security control service of the Cyber Security Center operated by the Ministry of

Table 1. Technological measures for server security

Classification	Security measure details
Blocking and prevention of intrusions	Establish and operate security devices, such as firewalls and intrusion detection systems
	Check for abnormal connections through periodical log analysis
	Inspect and monitor the application update server URL
Security control	Provide 24-hour security control
Server security	Apply password or authentication protection
	Encrypt and save user logs

Health and Welfare or the Ministry of Education, Science, and Technology.

2) Network security

Network security is designed to respond to and prepare against intrusions that could occur on the network. The network security standards corresponding to the mobile security level SL-3 consist of the physical and network classes. In the physical class, wireless LAN, Bluetooth, and tethering should be reviewed, and in the network class, safe network structures, firewalls, wireless intrusion prevention systems (WIPS), virtual private networks (VPN), and security control should be considered. The technological security measures that satisfy the network security requirements are shown in Table 2.

3G that has relatively robust security also belongs to the internet area. Directly connecting Wi-Fi that has relatively weak security with an internal network through partial service set identifiers (SSID) is a vulnerable construction in terms of security. If a Wi-Fi network is used to connect to an internal network, the risks posed by intrusions should be alleviated by actively handling the risks involved in a wireless LAN environment through wireless security solutions, such as WIPS. Additionally, potential intrusions of the wireless network can be routed towards the Internet network instead of the internal network. Whenever possible, implementing both methods would be ideal. In terms of preventing secondary damages from wireless network intrusions, it is structurally more secure to route all of the wireless APs such that they are initially connected to an external internet network and construct a Wi-Fi network in the same manner as the 3G or internet networks. In particular, the secure network structure in the network class should be designed based on the "Secure Network Structure by Security Level" suggested by the Security Standards.

As shown in Figure 2, the user accesses the access server in a smartphone demilitarized zone (DMZ) with a business mobile device to perform his or her tasks. The communication section is connected via VPN communication for VPN purposes. The smartphone access server processes the task queries transmitted by the business smartphone. The data updated in the process of processing the task queries are transmitted to the database (DB) server through the mediating server. The mediating server transmits the work data received from the smartphone access server to the DB server. The DB server stores the work data [8].

Regarding the connection via VPN, Clause 2 of Article 6 (access control system implementation and operation) of the "Standards for Measures to Warrant Security of Personal Information" specifies with regard to the protection of personal information that the "processor of personal information should apply secure means of access, such as VPN or a dedicated network, in cases where a personal information handler tries to access the personal information processing sys-

Table 2. Technological measures for network security

Classification	Security measure details
Wireless network connection	Block wireless LAN connections from unauthenticated equipment
	Block and detect illegal APs and ad hoc connections
	Block connections using services other than Wi-Fi and 3G (i.e., Bluetooth)
Work network linking	Configure separate servers for data and memo reports
	Block direct connections from the terminal-work network
Encryption of communication	Use safe encrypted communication channels (i.e., WPA2)
	Authenticate VPNs and generate secure channels

AP: access protocol, WPA: Wi-Fi protected access, VPN: virtual private network.

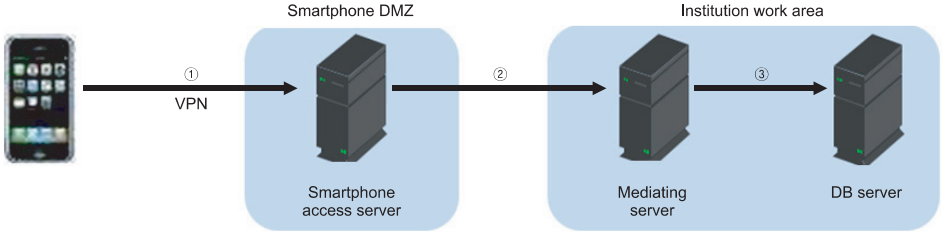

Figure 2. SL-3 network composition. DMZ: demilitarized zone, VPN: virtual private network.

http://dx.doi.org/10.4258/hir.2012.18.2.125

tem from the outside through a communications network." Thus, remote access through VPN is a principle to which the institutes interested in implementing a mobile EMR system should strictly adhere [12].

In conclusion, the desirable network composition for the efficient management of wireless networks is derived by forming a separate DMZ for smart terminals and only allowing access via VPN. In doing so, the access and administrative servers are placed in the DMZ for smart terminals and the mediating server is placed in the hospital work area.

3) Smart terminal security

Smart terminal security is designed to respond to device losses and potential intrusions. The security standards for smart terminals corresponding to the mobile security level SL-3 consist of user authentication, malware responses, data protection, mobile OS protection, resource management, and software management. With regard to user authentica-

Table 3. Security measures for smart terminals

Classification	Security measure details
User authentication	Block usage if an incorrect entry was made more than a certain number of times
	Detect password auto-lock setting
	Implement public authentication or an authentication solution of the equivalent security
Terminal authentication	Authenticate the terminal based on public authentication and distribute the key
	Authenticate the terminal based on device authentication and distribute the key
Application security	Implement a code signature by a trusted authentication institution
	Update exclusively via the telecommunications network
	Manage versions through PMS
	Perform the software-based (code signature) verification of application integrity
	Allow hardware (i.e., camera, GPS, and microphone) access only for approved software
Malware	Provide dedicated vaccine software
	Automatically detect and delete malwares when connecting to a mobile storage medium
	Force quit the session and record on the log if malignant behaviors are detected
Lost or stolen terminal	Implement remote locking and remote deletions
	Remotely track the terminal location
	Backup and restore mission-critical data
Platform security	Automatically detect platform structure modifications (i.e., jailbreaking and rooting)
	Implement the code-signature-based verification of platform integrity
	Implement logical privilege separation in the executive area (i.e., sandboxing)
	Verify the integrity of executive area memory
	Block or select control of the multi-tasking function
	Limit access privileges to the file system of the user processes
Remote control	Detect and restore modifications of the device configuration
	Remotely attest to the platform integrity
	Remotely attest to the application integrity
Connection management	Block wired and wireless direct connections between the smart terminal and PC
	Block tethering connections between the smart terminal and PC
	Install control systems for the media of smart terminals (i.e., micro SD) on the work PC
Document security	Allow attachment files to only be viewed as an image
	Prohibit screen captures of the work screen
	Encrypt transmitted documents and temporary documents
	Control access to document distribution via permitted N-screen

PMS: patch management system, GPS: global positioning system.

tion, the timing of the authentication execution, authentication method, and setting the clipping level to be taken in case of an authentication failure should be reviewed with respect to the basic lock setting. With regard to malware responses, the installation of mobile vaccine software should be considered. With regard to the protection of data stored in a smart terminal, storage medium control, screen capture prevention, and remote control in case of losses should be considered. Furthermore, the integrity of the mobile OS should be verified, and deformation should be detected; the application installation should be controlled and managed such that only permitted applications can be installed on a smart terminal. The technological security measures that satisfy the security requirements of these smart terminals are shown in Table 3.

User authentication necessitates a secure ID/password method that complies with the rules for password configurations or certificate methods. Here, the certificates must be saved in a secure space provided by the terminal. With regard to the password method, usage should be blocked if the password is not configured or is entered incorrectly more than a certain number of times, and it should be possible to determine whether the password auto-lock function is set up.

Device loss is one of the biggest vulnerabilities of mobile devices. Once lost, the terminal is out of the user's control. If a basic lock through a password configuration is not performed, the information stored in the mobile device will likely be leaked. If remote lock, remote control, and remote tracking functions are not supported or if the integrity of the mobile OS is not guaranteed because of jailbreaking or rooting, the use of a medical information system on a mobile device poses the risk of operating the service while ignoring critical risks. Furthermore, medical staff members should not be forced to use uniform devices simply for security reasons if they prefer diverse devices and platforms. Because most public medical institutions are set in bring your own device (BYOD) environment in which one's own devices are utilized for work, the terminals should be even more stringently managed [21].

Given that mobile devices provide computer-like functionalities by default, they can incur the same type of damage that PCs suffer from malwares. To overcome this problem, medical facilities should mandate the installation of vaccine programs for mobile devices, and automatic updates should be provided. If storage media (i.e., an SD card) is connected to a mobile device, the storage media should be automatically examined for malware, which should be deleted upon detection. Furthermore, if an abnormal connection or data transmission occurs, the session should be forced to quit, and the information on the session should be documented in a log. Medical facilities may refer to the "Guide to Using Smartphone Vaccine", which was written by the Korea Communications Commission (KCC) and the KISA for Korean smartphone users to form a safe environment for smartphone use, when addressing the use of vaccines for smart terminals. Regarding iOS-based smart terminals, this guide states that consumers using iPhones rarely suffer from malware infections because of Apple's security policy. Thus, a particular vaccine is not necessary. Android-based smart terminals are relatively more vulnerable to malware infections because of the open OS policy. Thus, smartphone vaccines must be installed for these terminals [22].

The mobile device management (MDM) solution is gaining attention as an effective solution to this comprehensive problem of smart terminals. In addition to satisfying the desire to use diverse devices and platforms, default MDM functions, such as the registration and management of terminals, remote terminal control in the case of losses, terminal control for the implementation of security policies, and the application distribution and configuration management, also allow all of the mobile devices and applications used at each facility to be managed effectively. As an essential element in legal compliance and the reinforcement of terminal security, the MDM solution should be seriously considered [21,23].

4) Managerial security

Managerial security standards corresponding to the mobile security level SL-3 consist of organizational security policies, facility security, software management, equipment management, and other aspects. Organizational security policies require dedicated policies for mobile device use and education as well as a committed person in charge of responding to incidents. Facility security requires secure control of the facilities with regard to the wireless LAN and mobile systems. Software management requires the security of mobile applications to be verified. Equipment management requires the development of guidelines for equipment management and periodic inspections of the wireless LAN system. In other standards, it must be confirmed whether all of the security products implemented as technology security measures obtained CC certification, and security verification must be requested to the authorities of the mobile system.

These managerial activities are often the most difficult part of mobile security because although a security solution can be established with the investment of funds, a significant amount of time and effort is required to prepare human resources, organizations, and policies that can operate them

http://dx.doi.org/10.4258/hir.2012.18.2.125

and effectively maintain and manage them. Besides the managerial security system undergoes constant changes because of the modification of the mobile system itself, changes in the security standards for mobile services, changes in external threats, discoveries of new vulnerabilities, and the advent of new mobile security technologies. To cope with these changes and maintain the proper security level medical facilities should analyze the effects of these changes, and risk management activities should be put in place to review new measures periodically. An information security management system (ISMS) is suggested for these managerial activities.

The K-ISMS (ISMS by KISA), G-ISMS (ISMS for e-Government), and ISO 27001 are common examples of ISMSs. The G-ISMS is the most appropriate system for public medical institutions. The G-ISMS was developed by the Ministry of Public Administration and Security and the KISA to rein-

Table 4. Managerial security system based on the ISMS

Classification	Substage	Contents
Security system establishment	Scope configuration	Define the security level for each task of the mobile EMR system and configure the application scope
	Policy/guideline establishment	Establish a security policy or internal guideline for the safe use of smart terminals according to the characteristics of the mobile system
	Establishment of the risk management plan	Identify the assets related to the mobile system, classify the threats and vulnerabilities that can affect the assets, and establish a risk management plan
	Risk analysis and assessment	Given the identified threats and vulnerabilities, asset values, and the possibility of failure for the security measures, analyze and evaluate the impact of the potential damage
	Risk handling	Given the risk acceptance level of the identified security threats and vulnerabilities, select appropriate measures and controls according to the results of the risk assessment
Security system implementation and operation	Establishment and implementation of security measure	Establish and implement security measures to execute the response and control actions selected in the risk-handling stage
	Security awareness education	Establish and execute appropriate security awareness education plans for mobile users
	Operation	Manage the operation status of the security system and report periodically
	Resource management	Manage resources to implement, operate, review, and improve the security system
Monitoring and review of the security system	Monitoring	Periodically monitor the security system
	Result assessment	Periodically review the security system and the achievements of the security measures
	Internal audit	Periodically execute an internal audit and renew and improve the security measures
Maintenance and improvement of the security system	Improvement activities	Continually improve the mobile security system by considering the security policies, security measures, audit results, case analysis, preventive measures, new security threats, and vulnerabilities
	Conference and sharing of opinions	Confer and share opinions with related parties about security system improvements
	Review of improvements	Confirm the accomplishment of the improvement goal

ISMS: information security management system, EMR: electronic medical record.

force the protection of the government's and public institutions' information and the citizens' personal information. The G-ISMS refers to the ISO 27001 and K-ISMS and indexes the assessment of the personal information protection levels at public institutions. The G-ISMS is useful for evaluating the information protection levels in the government and at public institutions and for effectively managing security [24,25]. Table 4 shows the managerial security system of the mobile EMR system established based on ISMS.

Managerial security includes all parts of the previously described sectional security reviews. It considers everything from whether the security measures for each section are well-established and operating to whether the newly emerging or changing laws or technologies are responded to in a timely manner and handled appropriately. With managerial security, attention from the medical facility's CEO, the consequent investments in human resources and costs, and company-wide participation are crucial.

IV. Discussion

In the age of smart health, a mobile EMR system is an essential element that can induce efficient improvements in consultation practices through a paradigm shift and bring the effects of improved medical services to patients. The transition into the smart health era has taken place, and the actors involved in mobile security and patient information protection should proactively prepare for this change. Security measures for protecting the valuable information of people, clientele, and patients are an issue that must be contemplated. A blueprint of a safe system that considers the mobile EMR system before this system is produced and applied throughout the production process is required. This blueprint should investigate the legal compliance issues as well as the technological and managerial considerations.

With regard to the establishment of a mobile EMR system, this paper intended to suggest a standard for locating and removing the threats that might arise through a preliminary risk analysis and that ultimately warrant continuous security by reflecting on the latest security issues.

Certainly, one will face realistic difficulties at the site in terms cost and time investments, but we hope that this paper has helped set up a clear direction and standards for medical institutions to follow. The most important thing is to establish mobile security policies that are appropriate for each institution to search for a cost-effective way of security controls, and to protect patient information.

A future study on the method of implementation after the application of security measures at actual medical facilities can be used as an illustrative case to determine the degree to which theory and reality correspond with one another.

Conflict of Interest

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

Acknowledgments

This work was supported by the Industrial Strategic Technology Development Program, 10038690, Global Healthcare Software Framework Development funded by the Ministry of Knowledge Economy (MKE).

References

1. Korea Communications Commission; Ministry of Public Administration and Security; Ministry of Knowledge Economy. National information security white paper. Seoul, Korea: Korea Communications Commission; 2011. p.278-9.
2. 148Apps.biz. App store metrics [Internet]. TrouserMac Industries; c2012 [cited at 2012 Feb 1]. Available from: http://148apps.biz/app-store-metrics/?mpage=catcount.
3. Ministry of Public Administration and Security. 2011 National informatization white paper. Seoul, Korea: Ministry of Public Administration and Security; 2011. p.323-6.
4. Min JH. The study of security measures of threat on mobile internet environment [dissertation]. Seoul, Korea: Konkuk University; 2010.
5. Jang SJ. IT planning series: the trend of mobile computing security technology. Seoul, Korea: National IT Industry Promotion Agency; 2011. p.12-20.
6. Ho AJ. Security of smartphone pouring. Inf Secur 21C 2010;114;54.
7. Park HW. Start to prepare the security, safe receipt of mobile office. Inf Secur 21C 2010;124;75.
8. National Intelligence Service. Security standards for smartphones for business use by national and public institutions. Seoul, Korea: National Intelligence Service; 2010.
9. Poon EG, Keohane CA, Yoon CS, Ditmore M, Bane A, Levtzion-Korach O, Moniz T, Rothschild JM, Kachalia AB, Hayes J, Churchill WW, Lipsitz S, Whittemore AD, Bates DW, Gandhi TK. Effect of bar-code technology on the safety of medication administration. N Engl J Med 2010;362:1698-707.

http://dx.doi.org/10.4258/hir.2012.18.2.125

10. Paoletti RD, Suess TM, Lesko MG, Feroli AA, Kennel JA, Mahler JM, Sauders T. Using bar-code technology and medication observation methodology for safer medication administration. Am J Health Syst Pharm 2007;64:536-43.
11. Ministry of Health and Welfare. Medical facility personal information protection guideline. Seoul, Korea: Ministry of Health and Welfare; 2010.
12. Ministry of Public Administration and Security. Notification of privacy impact assessment (2011-39). Seoul, Korea: Ministry of Public Administration and Security; 2011.
13. Korea Food and Drug Administration. Mobile PACS licensing examination guideline. Seoul, Korea: Korea Food and Drug Administration; 2011.
14. Choi MG. Security measures for safe use of wireless-LAN. Seoul, Korea: National Cyber Security Center; 2005. Report No.: NCSC-TR050021.
15. Hacking Response Team, Korea Internet and Security Agency. Wireless LAN security guide. Seoul, Korea: Korea Internet and Security Agency; 2010.
16. Center for Cyber Response, Financial Security Agency. Smartphone security guide in the banking sector. Seoul, Korea: Financial Security Agency; 2010. Report No.: FSA 2010-08.
17. Ministry of Public Administration and Security. Information system SW development security guide. Seoul, Korea: Ministry of Public Administration and Security; 2011. Reg. No.: 11-1311000-000330-10.
18. Ministry of Public Administration and Security. Information system establishment and operation guideline (2012-12). Seoul, Korea: Ministry of Public Administration and Security; 2012.
19. Public SW Security Team, Korea Internet and Security Agency. Mobile application security certification guide v1.0. Seoul, Korea: Korea Internet and Security Agency; 2011.
20. Ministry of Public Administration and Security. Standards for measures to warrant security of personal information (2011-43). Seoul, Korea: Ministry of Public Administration and Security; 2011.
21. Korea Communications Commission; Korea Internet and Security Agency. Guide to using smartphone vaccine. Seoul, Korea: Korea Communications Commission; 2011.
22. Park JH. The latest IT trend: the core of multiplatform mobile strategy, MDM solution. Seoul, Korea: National IT Industry Promotion Agency; 2012.
23. Min SS. Security threat of mobile office and MDM solution. Seoul, Korea: Financial Security Agency; 2011. Report No.: TM-01.
24. Kim YT. Issue report: information security and Introduction of personal information management framework. Seoul, Korea: Financial Security Agency; 2011. Report No.: vol. 2011-017.
25. Ministry of Public Administration and Security. The e-government ISMS certification guideline (2010-178). Seoul, Korea: Ministry of Public Administration and Security; 2010.