Guideline on Review and Approval for Cybersecurity of Medical Devices(For Industry)

November 2020

Ministry of Food and Drug Safety
Medical Device Evaluation Department

This guideline is intended to help understanding of applicants and represents the Ministry of Food and Drug Safety's (MFDS's) current thinking regarding the scope of medical devices that require cybersecurity and submissions on review and approval of those devices.

This guideline does not establish legally enforceable responsibilities. Please note that, despite some expressions contained herein (such as "shall (should)"), you are not required to comply with this guideline. In addition, this guideline has been prepared based on scientific and technical facts and statutes that are valid and effective as of Nov, 2019. The provisions in this Guideline are subject to change depending on the revision of the relevant statutes or specific factual developments.

※ Guideline for Industry refers to the description of legislation or administrative rules offered to industry to aid their understanding or the proclamation of the stance of regulatory authority in relation to certain civil affairs (Article 2 of the Regulations on the Management of Guidelines, etc. of the Ministry of Food and Drug Safety)

※ If you have any question or request regarding this guideline, please contact the Digital Health Device TF, High-tech Device Division, Medical Device Evaluation Department, National Institute of Food and Drug Safety Evaluation.

Tel : +82-43-719-3942~3949

Fax : +82-43-719-3940

Mail : medicaldevice@korea.kr

Table of Contents

I Overview

1. Background & Objective

With the advancement of information and communication technology, the medical devices with wire and wireless communications has been increased. Such medical devices are very diverse from “ubiquitous healthcare medical devices” intended for use in telemedicine to “implantable pacemakers” intended for use in life-sustaining purpose. It is expected that the type of medical devices with communications will be more diversified with this trends.

However, the importance of cybersecurity for medical devices is growing as cybersecurity threats such as hacking and information leakage are reported continuously and such threats could cause not only property loss but also direct harm to patient’s life.

Currently, manufacturers of medical devices are conducting risk management throughout the life cycle of medical devices from design stage to the use of medical devices in accordance with the Standards of Medical Device Good Manufacturing Practices. Patient’s risk related to cybersecurity infringement could be alleviated by applying risk management to cybersecurity for medical devices.

This guideline is intended to secure the safety management of medical devices with communications by clarifying the scope of medical devices required cyber security and submissions for the review and approval for them, and specifying security requirements applicable to the products by characteristics.

2. Scope

This guideline is established to ensure the cybersecurity of devices with wire and wireless communications, and the scope of the medical devices required cybersecurity is as follows:

1) Medical devices that send and receive personal health record such as biometric information of patients using wire and wireless communications.

2) Medical devices that can be controlled by using wire and wireless communications.

3) Medical devices required maintenance including firmware or software update via wire and wireless communications.

This guideline provides the minimum recommendations applicable to cybersecurity threats that could directly affect the health of users. In addition, it is recommended to comply with other applicable laws such as Medical Service Act and Personal Information Protection Act regarding the matters such as post-management and administrative security for users (medical institutions, etc.) or personal information leakage with no direct impact on the health of users.

3. Definitions

A. Availability

Function to provide Personal Health Record (PHR) immediately to authorized users and make sure that medical information exists when and where needed in the required form.

B. Personal Health Records

Personal information on patient's physical and mental condition with which a person is identifiable including the history of medical service provided and following information.

1) Patient registration information for providing medical service
2) Information on eligibility for patient care or payment
3) Numbers, symbols and other identifiers designated to identify patients for the purpose of providing medical service
4) Personal information collected from a patient to provide medical service
5) Information obtained through examination or test on body parts
6) Information on those who provide medical service (medical professionals, etc.) to a patient

C. Confidentiality

Function to make sure that personal health records is not disclosed to unauthorized parties or being used for unauthorized purposes

D. Respond

Activities to take actions on identified cybersecurity incident related to medical device

E. Standalone Software

Medical device software that has functions qualified for intended use of medical device as it is, and operates in an environment equivalent to general-purpose computer

F. Integrity

Function to prevent personal health records from being converted or destroyed in an unauthorized manner.

G. Protect

Activities to develop protective measures to secure cybersecurity in medical devices.

H. Recover

Activities to restore the function of medical device damaged by cybersecurity incident.

I. Cybersecurity

To keep the confidentiality, availability and integrity of information in cyber space.

J. Identify

Activities to identify and assess cybersecurity risks by a manufacturer to manage the cybersecurity risk of medical devices.

K. Encryption

A Technology to make people not to understand the information if they don’t know the decryption method by saving information after modifying it according to specific rules in an effort to keep information security.

L. Cybersecurity of Medical Device

Measures to prevent unauthorized use, rejection to use, misuse, modification and unauthorized access to personal health records that is saved, sent or received in medical device through wire and wireless communication, or program that controls such medical devices.

M. Detect

Proper activities that can detect the cybersecurity incident related to medical device

※ For terms related to risk management of medical devices, refer to Standards of Medical Device Good Manufacturing Practices (Ministry of Food and Drug Safety Notification) and Guideline on the Risk Management for Medical Devices (2007).

II General Principles of Cybersecurity in Medical Devices

Confidentiality, Integrity and Availability shall be considered for the cybersecurity of medical devices.

Confidentiality means to prevent personal health records from being disclosed to unauthorized parties or being used for unauthorized purposes. A manufacturer shall encrypt personal health records to make sure that the information is not easy to read even though the personal health records is exposed in the data transmission process or by illegal methods such as inquiry of the information by unauthorized person or error, and make sure that only authorized people can access the information and limit the level of access depending on the purpose and authority of users.

Integrity means to prevent personal health records from being converted or destroyed in an unauthorized way. Information should be accurate and complete and should not be distorted through forgery and falsification. Information modification should be done only by authorized users and log and modification history should be managed.

Availability means to provide personal health records immediately to authorized users and make sure that medical information exists when and where needed in the required form.

Confidentiality, integrity and availability are required to ensure cybersecurity of medical devices and they should be applied in the risk management process established in quality system by manufacturers in accordance with Standard for Manufacturing and Quality Management of Medical Devices as is the case of risk management of medical devices.

Risk management process of cybersecurity in medical devices has modular step from risk analysis, risk evaluation, risk control, evaluation of overall residual risk acceptability, risk management report and production to post-production information. Such cybersecurity risk

management shall be applied to medical device manufacturers who make medical devices with communications throughout the total product life cycle of information.

In the risk analysis stage of cybersecurity in medical devices, hazards to patient caused by destruction of confidentiality, availability and integrity is identified. In addition, potential impact from the realization of identified hazards shall be assessed and risk level shall be determined by evaluating the possibility of occurrence.

In the risk evaluation stage of cybersecurity in medical devices, decision should be made whether the risk calculated based on risk acceptance criteria defined in risk management plan for each identified hazard is low enough not to reduce risk.

In the risk control stage of cybersecurity in medical devices, appropriate control measures against cybersecurity risk shall be taken considering the result of risk evaluation, and all controls necessary to implement the measures shall be determined and executed. In addition, the evaluation of acceptability of overall residual risk shall be conducted after applying risk control measures. Manufacturers shall record a series of procedures regarding risk management process of cybersecurity in risk management report. In the information stage of production and post-production, systematic procedures shall be established and maintained to review the information on cybersecurity.

In addition, manufacturers shall establish the goals of cybersecurity with appropriate functions and levels to apply the risk management process of cybersecurity. Cybersecurity goals shall be in line with cybersecurity policies, and achievable and measurable at a feasible level, considering applicable cybersecurity requirements, risk assessment and risk treatment results. In addition, a manufacturer shall collect and analyze opinion from internal and external customers and incorporate them in risk management of cybersecurity in medical devices continuously throughout the total product life cycle of medical devices.

[Figure 1. Risk Management Process of Cybersecurity in Medical Devices]

III Scope & Requirements of Medical Devices required Cybersecurity

1. Definition and Classification of Cybersecurity Safety for Medical Devices

Safety level and requirements of cybersecurity in medical devices with wire and wireless communications can be different depending on the level of harm which can be caused by potential defects from cybersecurity violations and affect to users.

The cybersecurity safety level for medical devices can be divided into three as shown in the table 1 below: major, moderate and minor.

Level ‘Major’ refers to the case where medical device cybersecurity breaches could cause serious injury or death, permanent impairment of body function or possibility of permanent damage to body structure. Level ‘Moderate’ refers to the case where users suffer from temporary and minor injuries and need medical intervention. Level ‘Minor’ refers to the case where users experience temporary discomfort or suffer from reversible, minor and short-term discomfort without the need for medical intervention.

[Table 1. Classification of Cybersecurity Safety Level for Medical Devices]

Classification	Definition
major	Medical device cybersecurity breaches could cause serious injury or death, permanent impairment of body function and possibility of permanent damage to body structure.
moderate	Medical device cybersecurity breaches could cause temporary and minor injury to users and medical intervention may be necessary.
minor	Medical device cybersecurity breaches could cause temporary discomfort or reversible, minor and short-term discomfort to users without the need for medical intervention

Medical devices that fall under ‘Major’ level are mainly Class IV medical devices (implantable medical device, etc.) that could cause severe injury or death due to cybersecurity breaches and some Class II and III medical devices that could cause permanent impairment of body function and permanent damage to body structure due to cybersecurity breaches such as surgical medical devices, medical devices using radiation for treatment, medical devices for life supporting and medical devices for measuring vital signs which could impact life of patients if alarm or warning sign is missed.

Medical devices that fall under ‘Moderate’ level are mainly Class II and III medical devices for treatment that could cause temporary and minor injury or need for medical intervention due to medical device cybersecurity breaches and Class II medical devices including medical devices for sending and receiving vital signs, medical devices for measuring vital signs and medical devices for analysis and diagnosis, which could lead to wrong treatment, deprivation of treatment opportunities or possibility of treatment delay due to forged or missing vital signs or results of vital signs analysis and diagnosis due to cybersecurity breaches.

Medical devices that fall under ‘Minor’ level are medical devices which could cause temporary discomfort or reversible, minor and short-term discomfort without the need for medical intervention due to cybersecurity breaches. Class II medical devices which are not intend to treat, monitor, analyze or diagnose and Class I medical devices fall into this category.

The procedures to determine safety level of cybersecurity and examples of classification are shown in Table 2, and items in the example may be different depending on the intended use and communication technology applied (wire, wireless, Near Field Communication, Telecommunication, etc.)

[Table 2. Classification of Safety Level of Cybersecurity and Examples]

Level	Definition	Classification	Examples of Items
Major	Cases where medical device cybersecurity breaches could cause serious injury or death, permanent impairment of body function and possibility of permanent damage to body structure	Class IV medical devices	Implantable defibrillator , Implantable pacemaker, Implantable insulin pump, U-healthcare implantable insulin pump, Implantable analgesic simulator , Insulin infusion pump, etc.
		Following medical devices among Class II and III.	
		Medical devices for operation in which malfunction can occur with cybersecurity breach	Robotic surgical system[3], Laser surgical instrument[3], Electrosurgical system[3], etc.
		Medical devices using radiation for treatment in which malfunction can occur with cybersecurity breach	Accelerator system collimator electron applicator[3], Therapeutic medical neutron irradiation device[3], Therapeutic X-ray irradiation device[3], etc.
		Medical device that could impact the life of patients due to malfunction caused by cybersecurity breach	Low-powered defibrillator [3], High-powered defibrillator [3], etc.

		Medical devices for Life-supporting in which malfunction can occur with cybersecurity breach	Ventilator for general purpose[3], Ventilator for home-use [3], Patient monitoring system (at all times)[2] etc.
		Medical devices for measuring vital signs which could impact the life of patients due to missed alarm or warning caused by cybersecurity breach	Patient monitoring system[2], etc.
Moderate	Cases where medical device cybersecurity breaches could cause temporary and minor injury to users and medical intervention may be necessary	Class III medical devices	Intense pulsed light generator, Extracorporeal shock wave treatment system, Computer aided diagnosis system, U-health diagnosis support system, U-healthcare glucose meter, Blood glucose meter for self-test, etc.
		Class II medical devices	Ultrasound vibrator, Ultraviolet Phototherapy unit, Heater System, Telemetry system transmitter, Computer aided detection system, U-healthcare medical devices, Ultrasound imaging system, MRI system, Microarray chip analyzer, Stereotaxic navigation unit, Hyperbaric chamber for medical use, etc.

Minor	Cases where medical device cybersecurity breaches could cause temporary discomfort or reversible, minor and short-term discomfort to users without the need for medical intervention.	Medical devices that are intended to treat, monitor, analyze or diagnose among Class II medical devices	Electronic thermometer, Automatic electronic sphygmomanometer, Light source for endoscopy, Dry heat sterilizer, Medical UV sterilizer, Medical water sterilizer, Electric wheelchair, Electronic goniometer for medical care, Cell washing centrifuge, Refrigerator for blood Treatment table and chair for ear, nose and throat, Alkali water producing equipment, etc.
		Class I medical devices	U-healthcare gateway, Protein analyzer, Lactate analyzer, etc.

2. Requirements for Cybersecurity of Medical Devices

The requirements for cybersecurity of medical devices shall be applicable to total product life cycle of medical devices from design to use and divided into ‘Identify’, ‘Protect’, ‘Detect’, ‘Respond’ and ‘Recover’ stages.

‘Identify’ refers to the process where a manufacturer identifies and assesses cybersecurity risks in an effort to manage cybersecurity risk of medical devices including evaluation activities of cybersecurity risk.

‘Protect’ refers to the process where protective measures are developed to ensure cybersecurity of medical devices and measures such as access control, education, training and data security are applied.

‘Detect’ refers to appropriate activities that can detect the outbreak of medical device cybersecurity incident and ‘detect’ can be done through measures including continued cybersecurity monitoring.

‘Respond’ refers to activities necessary to take actions on detected cybersecurity incident and includes security treat analysis and mitigation measures.

Finally, ‘Recover’ stage refers to activities to restore the function of medical devices damaged by cybersecurity incident and includes the establishment of a recovery plan.

A manufacturer can determine cybersecurity safety level for its medical device according to <Table 2> and apply relevant cybersecurity requirements.

However, the following requirements are established incorporating technical features of products which are currently in use and some of the cybersecurity requirements may be excluded or added if new products are developed in the future or there is any differences in characteristics of communication. Such requirements shall be incorporated into a product through continued post-management after getting approval of the product

In addition, it is recommended to apply following requirements in Table 3 throughout the risk management activities considering technical characteristics of the products even though some requirements are not applicable to a certain safety level.

[Table 3. Requirements for Cybersecurity of Medical Devices]

No.	Classification	Item	Requirements	Applicable scope (level)		
				Major	Moderate	Minor
1	'Identify' and 'Protect'	Access control and Authentication	It shall be possible to give access authority depending on user's role (of medical devices) based on identification and authentication and make the user access only authorized data.	◦	○	△
2		Prohibiting multiple access	The same user shall not have multiple access.	○	○	△
3		Recognition of User access (of medical devices)	The access by unauthorized users (of medical devices) shall be recognized and distinguished.	○	○	△
4		Limiting the access of unauthorized users (of medical devices)	The access by unauthorized users (of medical devices) shall be blocked.	○	○	△
5		Blocking unauthorized network communication	Communication access of Unauthorized network shall be limited.	○	○	△
6		Blocking remote access	If users (of medical devices) can access the server of a medical institution, access control shall be given not to access to server in case where the user account or the medical devices be stolen.	○	○	○
7		Authentication management of users (of medical devices)	The expiration date of the users (of medical devices) account can be established and access shall be blocked after the set period of time.	○	○	△
8		Auto session close	Communication among medical devices or access shall be closed after the set period of time.	○	○	△
9		Strengthening rules on creating passwords.	Rules on creating passwords shall be satisfied the 'Standard for Technical and Administrative Measures to Protect Personal Information'	○	○	△
10		Prohibiting password hardcoding	Hardcoding of password shall not be recommended.	○	○	△
11		Prohibiting password exposure	Password shall be used in a way not to expose password such as using ***.	○	○	△

12		Approval for firmware or software update	There shall be a procedure to request or check approval from administrator upon firmware or software update or such update shall be executed in a way to ensure security at a distance where administrator or user can recognize.	○	○	○
13		Ensuring the integrity of firmware or software update	Upon distributing firmware or software update file, version shall be identified and distributor and integrity of the file shall be verified.	○	○	○
14		Using authentication method upon firmware or software update	Firmware or software update shall be limited to authorized code including check for code signing	○	○	○
15		Ensuring the confidentiality and integrity for transferring control information of medical devices on network	In case where control information of medical devices is communicated through network, confidentiality and integrity shall be ensured by using appropriate encryption and decryption methods.	○	○	△
16	'Identify' and 'Protect'	Ensuring the confidentiality and integrity for transferring personal health records on network	In case where personal health records is communicated through network, confidentiality and integrity shall be ensured by using appropriate encryption and decryption methods.	○	○	△
17		Using safe encryption algorithm	Encryption algorithm used for sending and storing data shall use verified encryption algorithm or module with security level of 112-bit or higher and encryption key used for encryption shall be managed safely.	○	○	△
18		Minimizing physical infringement on communication port	Physical locking shall be provided to minimize communication port infringement.	○	○	△
19		Removing or inactivating unnecessary services	In case of setting default value as inactivation of services including unnecessary access from external port, additional security measures such as setting password and IP restriction shall be conducted.	○	○	△
20		Managing personal health records storage	It is recommended not to store personal health records in measuring device or gateway used outside of medical institutions.	○	○	△

21		Recording system log for data audit	When a user accesses medical device, logs such as access log, patient information inquiry and generation, modification and deletion of data shall be recorded.	○	○	△
22	'Detect', **'Respond'** and 'Recover'	Verification for major execution and setting files and taking actions	Integrity of major execution and setting files shall be verified to ensure the normal operation of medical devices and countermeasures shall be considered if integrity error occurs.	○	○	△
23		Providing information on countermeasures to be taken when cybersecurity treat is detected	Emergency contact and information of device manufacturer for consultation shall be provided to handle cybersecurity incident that may occur during the use of medical device and measures to be taken when cybersecurity threat is detected shall be established and provided to users.	○	○	○
24		Protection against DDoS attack	Countermeasures to respond to DDoS attack shall be in place for devices which access public network to control medical device in real time, or send and receive information that could be directly related to patient's life (ex: information that belongs to cybersecurity safety level 'Major') in real time.	○	△	△

※ Requirement 18 'Minimizing physical infringement on communication port and Requirement 21 'Recording system log for data audit' may not be applied to implantable medical devices.

IV Submissions for Review and Approval

1. Scope and Requirements of Submissions

‘Submissions on Software Verification and Validation’ shall be submitted among documents required under Article 29(8) (Requirements of Attached Information) of the Regulation on Medical Device Approval/Reporting/Review, Etc. (Ministry of Food and Drug Safety Notice) upon application for the approval for medical devices with wire and wireless communications.

The documents to be submitted shall incorporate the requirements for cybersecurity of medical devices in Table 3 as a measure to prevent forgery/falsification of information, malfunction or unauthorized access to medical devices. In case, however, where some requirements need to be excluded or modified for application based on the risk analysis by a manufacturer, test standard and its ground shall be submitted in accordance with subparagraph 4 of Article 26(1) of the regulation and as an evidence document, ‘Cybersecurity Risk Management Document’ and ‘Checklist for Essential Principles of Cybersecurity of Medical Devices’ in Table 4 may be submitted.

‘Checklist for Essential Principles of Cybersecurity of Medical Devices’ is to check whether requirements for cybersecurity of medical devices are met and one shall fill out the form depending on the characteristics of a product for review and approval for medical devices.

‘Documents on Cybersecurity Risk Management’ and ‘Documents on Software Verification and Validation’ are the supporting documents showing that the applied medical device meets the cybersecurity requirements included in the ‘Checklist for Essential Principles of Cybersecurity of Medical Devices’.

‘Documents on Cybersecurity Risk Management’ is a report designed to record risk

management activities to minimize and prevent potential harm by identifying hazards related to cybersecurity throughout the total product life cycle of medical devices. The identification of the cybersecurity risks of the applied product and the results of risk analysis and risk reduction measures for each risk shall be described in the report.

‘Documents on Software Verification and Validation’ are objective data that can verify the result of the actions to control risks identified in the medical device risk management process. The documents shall include test and verification process for the cybersecurity requirements, test result, and re-test results in case where software was changed during testing and verification.

Preparation for ‘Documents on Cybersecurity Risk Management’ and ‘Documents on Software Verification and Validation’ can be referred to Guideline on the Preparation for Risk Management in Summary Technical Documentation for Medical Devices (2014) and Guideline on Review and Approval for Software as Medical Devices (2015).

2. Checklist for Essential Principles of Cybersecurity of Medical Devices

Upon filling out the ‘Checklist for Essential Principles of Cybersecurity of Medical Devices’, the name, cybersecurity safety level (major, moderate, minor) and information of medical devices regarding the characteristics of communication such as communication technology (wire or wireless communication, communication method, etc.) and intended use of communication (controlling medical device, monitoring vital sign, etc.) shall be written down.

Based on the information written in the checklist, information such as requirements for each cybersecurity safety level, verification method of conformity, applicable laws and standards, attachments and document number shall be written down

Depending on the technical characteristics of the product, requirements may be excluded or added. In case where requirements are excluded, fill out justifiable reasons in ‘Verification method of conformity ’field, and in case where requirements are included, one may add the requirements to existing checklist. For example, in case of software as medical devices for standalone, security requirements which can be applied only to hardware may be excluded and if control measures can be taken against security threat with software, relevant requirements may be added

[Table 4. Checklist for Essential Principles of Cybersecurity of Medical Devices]

< Description of Characteristics of Medical Device of Cybersecurity >
1) Cybersecurity safety level: □ Major □ Moderate □ Minor
2) Communication technology used:
3) Purpose of communication: □ Sending and receiving personal health records such as biometric information of patient
□ Device control
□ Maintenance such as firmware or software update
4) Whether public network is connected or not:

Essential Principles of Cybersecurity of Medical Devices	Whether the device is subject to requirements	Verification method of conformity	Applicable laws and standards	Attachments or document number
1. ‘Identify’ and ‘Protect’				

1.1 Access control and authentication It shall be possible to give access authority depending on user's role (of medical device) based on identification and authentication and make the user access only authorized data.				
1.2 Prohibiting multiple access The same user shall not have multiple access.				
1.3 Recognizing Users (of medical devices) access The access by unauthorized users (of medical devices) shall be recognized and distinguished.				
1.4 Limiting the access of unauthorized users (of medical devices) The access by unauthorized users (of medical devices) shall be blocked.				
1.5 Blocking unauthorized network communication Unauthorized network communication access shall be limited.				
1.6 Blocking remote access If users (of medical devices) can access the server of a medical institution, access control shall be given not to access to server in case where the user account or the medical devices be stolen.				
1.7 Authentication management of users (of medical devices) The expiration date of the users (of medical devices)) account can be established and access shall be blocked after the set period of time				
1.8 Auto session close Communication among medical devices or access shall be closed after the set period of time				
1.9 Strengthening rules on creating passwords Rules on creating passwords shall satisfy the 'Standard for Technical and Administrative Measures to Protect Personal Information'				
1.10 Prohibiting passwords hardcoding Hardcoding of password shall not be recommended				
1.11 Prohibiting password exposure Password shall be used in a way not to expose password such as using ***.				

1.12 Approval for firmware or software update There shall be a procedure to request or check approval from administrator upon firmware or software update or such update shall be executed in a way to ensure security at a distance where administrator or user can recognize				
1.13 Ensuring the integrity of firmware or software update Upon distributing firmware or software update file, version shall be identified and distributor and integrity of the file shall be verified.				
1.14 Using authentication method upon firmware or software update Firmware or software update shall be limited to authorized code including check for code signing.				
1.15 Ensuring the confidentiality and integrity for transferring medical device control information on network In case where medical device control information is communicated through network, confidentiality and integrity shall be ensured by using appropriate encryption and decryption methods.				
1.16 Ensuring the confidentiality and integrity for transferring personal health records on network In case where personal health records is communicated through network, confidentiality and integrity shall be ensured by using appropriate encryption and decryption methods.				
1.17 Using safe encryption algorithm Encryption algorithm used for sending and storing data shall use verified encryption algorithm or module with security level of 112-bit or higher and encryption key used for encryption shall be managed safely.				
1.18 Minimizing physical infringement on communication port Physical locking shall be provided to minimize infringement on communication port				
1.19 Removing or inactivating unnecessary services In case of setting default value as inactivation of services including unnecessary access from external port, additional security measures such as setting password and IP restriction shall be conducted.				

1.20 Managing personal health records storage It is recommended not to store personal health records in measuring device or gateway used outside of medical institutions.				
2. 'Detect', 'Respond' and 'Recover'				
2.1 Recording system log for data audit When accessing medical devices of users, logs such as access log, patient information inquiry and generation, modification and deletion of data shall be recorded.				
2.2 Verifying integrity of major execution and setting files and taking actions Integrity of major execution and setting files shall be verified to ensure the normal operation of medical devices and countermeasures shall be considered if integrity error occurs.				
2.3 Providing information on countermeasures to be taken when cybersecurity treat is detected Emergency contact and information of device manufacturer for consultation shall be provided to handle cybersecurity incident that may occur during the use of medical device and measures to be taken when cybersecurity threat is detected shall be established and provided to users.				
2.4 Protection against DDoS attack Countermeasures to respond to DDoS attack shall be in place for devices which access public network to control medical device in real time, or send and receive information that could be directly related to patient's life (ex: information that belongs to cybersecurity safety level 'Major') in real time.				

V References

1. Standard for Technical and Administrative Measures to Protect Personal Information, Korea Communications Commission Notice, Ministry of the Interior and Safety
2. Guideline on the Review and Approval for U-healthcare Medical Devices System, Ministry of Food and Drug Safety (2013)
3. Guideline on the Review and Approval for Software as Medical Devices (2015)
4. Guideline on Risk Management of Medical Devices, Ministry of Food and Drug Safety (2007)
5. Guideline on IOT for Home and Appliances, Korea Internet & Security Agency (2017)
6. Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, FDA (2014)
7. Framework for Improving Critical Infrastructure Cybersecurity, NIST (2014)
8. ISO 14971, Medical devices - Application of risk management to medical devices (2007)
9. ISO 13485, Medical devices - Quality management systems – Requirements for regulatory purposes (2016)
10. KS X ISO/IEC 27000, Information Technology-Security Technique- Information Protection Management System- Overview and Terminology (2014)
11. KS X ISO/IEC 27001, Information Technology-Security Technique -

Information Protection Management System- Requirements (2014)

12. KS X ISO/IEC 27002, Information Technology-Security Technique - Practical Guideline on Information Protection Management (2014)
13. KS X ISO/IEC 27032, Information Technology-Security Technique - Guideline on Cybersecurity (2014)
14. KS X IEC TR 80001-1, Application of Risk Management for IT Network where Medical Devices are Integrated–Part 1: Roles, responsibilities and activities (2012)
15. KS X IEC TR 80001-2-1, Application of Risk Management for IT Network where Medical Devices are Integrated–Part 2-1: Modular risk management for medical IT network- practical applications and examples (2015)
16. KS X IEC TR 80001-2-2, Application of Risk Management for IT Network where Medical Devices are Integrated–Part 2-2: Guideline on security requirements for medical devices, disclosure of risks and control and communication (2015)
17. KS X IEC TR 80001-2-3, Application of Risk Management for IT Network where Medical Devices are Integrated–Part 2-3: Guideline on wireless network
18. Postmarket Management of Cybersecurity in Medical Devices, FDA (2016)

(Digital Health Devices Task Force) High-tech Medical Devices Division, Medical Device Evaluation Department
National Institute of Food and Drug Safety Evaluation

187, Osongsaengmyeong 2-ro, Osong-eup, Heungdeok-gu, Cheongju-si, Chungcheongbuk-do (28159)

TEL: +82-43- 719-3942~3949 FAX: +82-43-719-3940

medicaldevice@korea.kr

http://www.mfds.go.kr/medicaldevice

Ministry of Food and Drug Safety

Medical Device Evaluation Department