Provisional Translation (as of November 2023)[*]

PSEHB/MDED Notification No.0331-8
March 31, 2023

To: Directors of Prefectural Health Departments (Bureaus)

Director of the Medical Device Evaluation Division,
Pharmaceutical Safety and Environmental Health Bureau,
Ministry of Health, Labour and Welfare
(Official seal omitted)

Application of Article 12, Paragraph 3 of Essential Principles for Medical Devices

The standard for medical devices specified by the Minister of Health, Labour and Welfare pursuant to the provisions of Article 41, Paragraph 3 of the Act on Securing Quality, Efficacy and Safety of Products including Pharmaceuticals and Medical Devices (Ministerial Notification No. 122 of 2005; hereinafter referred to as the "Essential Principles") has been partially revised by the "Partial Revision of Standards for Medical Devices Specified by the Minister of Health, Labour and Welfare pursuant to the provisions of Article 41, Paragraph 3 of the Act on Securing Quality, Efficacy and Safety of Products including Pharmaceuticals and Medical Devices" (Ministerial Notification No. 67 of 2023). Article 12, Paragraph 3, which is stipulated in the partially revised Essential Principles shall be applied on April 1, 2023. A transitional measure period of one year has been established. For the medical devices that must comply with Article 12, Paragraph 3 of the revised Essential Principles, the provisions then in force shall remain applicable until April 1, 2024.

The handling of these issues is as follows. Please inform thoroughly the relevant organizations and the related holders of marketing authorization under your supervision.

Please note that copies of this notification will be sent to the President of the Pharmaceuticals and Medical Devices Agency, the President of the Japan Federation of Medical Devices Associations, the President of the American Medical Devices and Diagnostics Manufacturers' Association, the Chairman of the Medical Equipment Committee of European Business Council in Japan, the Chairman of the IVD Committee of European Business Council in Japan, the Chairman of the Japan Association of Clinical Reagents Industries and the President of the

[*] This English version of the Japanese Notification is provided for reference purposes only. In the event of any inconsistency between the Japanese original and the English translation, the former shall prevail.

Association of Registered Certification Bodies under PAL.

***

1. Purpose of Article 12, Paragraph 3 of the Essential Principles

The Essential Principles stipulate the fundamental requirements for quality, efficacy, and safety that medical devices should fulfill, and require that risk management is applied to medical devices to reduce the risk to an acceptable level.

Necessary measures for cybersecurity have been already requested in MHLW† Notifications such as "Ensuring Cybersecurity in Medical Devices" (PFSB/ELD Notification No. 0428-1 and PFSB/SD Notification No. 0428-1 dated April 28, 2015) and "Guidance on Ensuring Cybersecurity of Medical Devices" (PSEHB/MDED Notification No. 0724-1 and PSEHB/PSD Notification No. 0724-1 dated July 24, 2018). With the recent publication of the "Principles and Practices of Medical Device Cybersecurity" by the International Medical Device Regulators Forum (IMDRF) in March 2020 (hereinafter referred to as IMDRF N60 Document), based on the IMDRF N60 Documents and the IMDRF N47 Documents (Essential Principles of Safety and Performance of Medical Devices and IVD Medical Devices), the Essential Principles has been revised to add Article 12, Paragraph 3 to incorporate following three aspects of design, manufacture and life cycle activities for ensuring cybersecurity for medical devices using software:

1) plan to ensure cybersecurity of medical devices throughout the total product life cycle;
2) design and manufacture to reduce cyber risks; and
3) establishment of minimum requirements for hardware, networks, and IT security measures required for the environment of appropriate operation.

2. Key points and interpretation of Article 12, Paragraph 3 of the Essential Principles

(1) "medical devices using software that are used in connection with other devices and networks, etc." refers to medical devices that exchange electromagnetic information by connecting to other devices (medical devices, IoT devices, peripheral devices or external storage media (USB memory, SD card, HDD, CD, DVD, etc.)), Electronic Medical Records (EMRs), PCs (including PCs brought in from outside), networks (in-hospital systems, out-of-hospital systems, and global), etc.

(2) "external unauthorized access and attack, etc." assumes malicious unauthorized access using methods that are not anticipated by the designer in normal use, such as targeting vulnerabilities, intentional overload attacks (DoS(Denial of Service) Attack or DDoS (Distributed Denial of Service) Attack, etc.), and access by attacks intended to infect

† The term "MHLW" refers to the "Ministry of Health, Labour and Welfare."

malware (malicious software). As cyber attacks have become increasingly diverse and sophisticated in recent years, it may be necessary to address other types of attacks in the future.

(3) "appropriate requirements shall be identified, taking into account the operating environment and network use environment of the medical device" refers to identifying the operating environment such as medical institution, home, emergency and operating environment for implantable devices etc. as well as other elements such as the type of network to be connected, the operating system and platforms including various libraries, etc., and establishment of appropriate requirements for the intended use of medical devices, including the operational framework suitable for the operating environment.

(4) "the risk related to cybersecurity that may affect the function of the medical device or cause safety concerns shall be identified and evaluated, and risk management shall be conducted to reduce such cyber risks" means to appropriately manage cybersecurity-related risks as well as other risks and identify cybersecurity vulnerabilities, evaluate risks associated with threats and adverse effects resulting from exploiting such vulnerabilities, and appropriately control risks, as shown in JIS T 81001-5-1, for example.

(5) "such medical devices shall be designed and manufactured based on a plan to ensure cybersecurity throughout the total product life cycle of the medical device" refers to design and manufacturing to ensure cybersecurity throughout the entire life cycle, taking into account not only efforts in the design and manufacturing process, but also plans for collaboration with medical institutions and countermeasures to address vulnerability (including post-market updates, etc.), so that ensuring cybersecurity can be achieved, and cybersecurity issues or vulnerabilities can be addressed when they are found.

3. Application of Article 12, Paragraph 3 of the Essential Principles and Confirmation of Conformity

(1) For medical devices using software, market authorization holders of the medical device, persons with special approval for foreign-manufactured medical device or foreign manufacturers of designated specially-controlled medical devices (hereinafter referred to as MAH) have been already required to ensure the safety and essential performance of medical devices by implementing appropriate risk management throughout the entire life cycle of medical device software according to JIS T 2304. In addition, for medical devices using software, it is necessary to further strengthen cybersecurity measures through efforts in the product life cycle according to JIS T 81001-5-1 to reduce cybersecurity risks to an acceptable level and prevent the occurrence and spread of patient harm.

※ JIS T 81001-5-1 (Health software and health IT systems safety, effectiveness and security －Part 5-1: Security－Activities in the product life cycle) describes the cybersecurity measures to be implemented by the manufacturer in addition to the requirements for the product lifecycle as specified in JIS T 2304 (Medical device software－Software life cycle processes).
(Note for English version: These standards are identical with corresponding international standards, IEC 81001-5-1 and IEC 62304 respectively.)

(2) Other than JIS T 81001-5-1, the conformity with Article 12, Paragraph 3 of the Essential Principles may be confirmed by conformity to appropriate standards, etc. used internationally for ensuring cybersecurity of medical devices using software, such as IEC 81001-5-1. When applying for approval (including applications for partial changes in approval, the same shall apply hereinafter) or certification (including applications for partial changes in certification, the same shall apply hereinafter), explain the appropriateness of using these alternative standards, etc.

(3) The MAH shall establish a system that appropriately considers and implements the confirmation and verification of the cybersecurity of medical devices using software, and appropriately records and retains the implementation of the confirmation, etc., regarding compliance. Data shall be presented and appropriate explanations shall be provided at the request of the person authorized to investigate pursuant to the provisions of Article 23-2-5, Paragraph 7 or Article 23-2-23, Paragraph 4 of the Act on Securing Quality, Efficacy and Safety of Products including Pharmaceuticals and Medical Devices (Law No. 145 of 1960).

(4) MAH applying for approval or certification of specially-controlled medical devices or controlled medical devices must attach data showing conformance to JIS T 81001-5-1 etc. The conformity of general medical devices should be confirmed in the same manner, but data are not required to be attached when submitting a notification.

4. Transitional Measures

Article 12, Paragraph 3 of the Essential Principles added by this revision shall apply as of April 1, 2023, but may remain in force until March 31, 2024.

(1) Medical devices approved or certified or notified on or before March 31, 2024, to which the revised Essential Principles apply, shall not be required to be applied or notified again.

However, if it is necessary to apply for approval of the medical device or partial change in the matters to be approved or notified after April 1, 2024, due to any change in the matters to be approved or notified, attach data showing compliance with the revised Essential Principles after confirming compliance with the revised Essential Principles.

For medical devices to be marketed after April 1, 2024, it is necessary to verify compliance with the revised Essential Principles, and to be able to present data on compliance with the revised Essential Principles when requested.

Handling of medical devices manufactured and marketed on or before March 31, 2024, shall be notified later.

(2) For medical devices for which applications for approval, certifications, or notifications are submitted on or before March 31, 2024, it is not necessary to attach data showing compliance with the revised Essential Principles when applying for approval, applying for certification, or submitting notifications.

The provision in 4. (1) shall apply mutatis mutandis to the handling of the data after April 1, 2024.

(3) For medical devices that submit applications for approval or certifications after April 1, 2024, it is necessary to attach data on compliance with the revised Essential Principles after confirming compliance with the revised Essential Principles. For medical devices to be notified, the conformity to the revised Essential Principles shall be confirmed.