PSB/MDED Notification No. 0328-1
PSB/PSD Notification No. 0328-3
March 28, 2024

To: Directors of Prefectural Health Departments (Bureaus)

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

Management of Vulnerabilities to Ensure Cybersecurity of Medical Devices

For ensuring cybersecurity of medical devices, the notification “Ensuring Cybersecurity in Medical Devices” (PFSB/ELD Notification No. 0428-1 and PFSB/SD Notification No. 0428-1, issued jointly by the Counsellor (Evaluation and Licensing of Medical Devices/Regenerative Medical Products) of Minister's Secretariat, Ministry of Health, Labour and Welfare (hereinafter referred to as MHLW) and by the Director of the Safety Division, Pharmaceutical and Food Safety Bureau, dated April 28, 2015) requires appropriate cybersecurity risk management for medical devices to ensure the safe use of medical devices. In addition, based on the activities in the international framework for the purpose of international harmonization of cybersecurity measures by the International Medical Device Regulators Forum (IMDRF), such as the issuance of the “Principles and Practices for Medical Device Cybersecurity (hereinafter referred to as the “IMDRF/CYBER WG/N60 Guidance”),” for the purpose of introducing and developing the technical requirements including the international resistance standards against cyber-attacks on medical devices in Japan, the development goals, technical requirements, etc., which are necessary for cybersecurity of medical devices, were discussed. They were compiled primarily as the “Guidance for the Introduction of Cybersecurity of Medical Devices” for medical device marketing authorization holders (hereinafter referred to as MAHs) , and it was informed by the “Guidance for Ensuring Cybersecurity of Medical Devices and

Thorough Implementation” (Joint PSEHB/MDED Notification No. 1224-1 and PSEHB/PSD Notification No. 1224-1, dated December 24, 2021, issued jointly by the Directors of the Medical Device Evaluation Division and the Pharmaceutical Safety Division of the Pharmaceutical Safety and Environmental Health Bureau, MHLW). In addition, following the issuance of a supplement guidance by the IMDRF, the handling of the Software Bill of Materials (SBOM), the handling of legacy medical devices, correction of vulnerabilities, incident response, etc. were considered based on the supplement guidance. Then, the revised version of the “Guidance for the Introduction of Cybersecurity of Medical Devices” was presented in the “Revision of the Guidance for the Introduction of Cybersecurity of Medical Devices” (Joint PSEHB/MDED Notification No. 0331-11 and PSEHB/PSD Notification No. 0331-4, dated March 31, 2023, issued jointly by the Directors of the Medical Device Evaluation Division and the Pharmaceutical Safety Division of the Pharmaceutical Safety and Environmental Health Bureau, MHLW). In order to further strengthen the measures against the cyber-attacks on medical devices conducted across borders and to ensure the safety in medical settings, the MHLW revised the “Standards for Medical Devices Specified by the MHLW 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” (MHLW Ministerial Announcement No. 122 of 2005) to construct an approval and licensing system that can confirm the cybersecurity measures for medical devices.

This time, in order to smoothly secure the systems of the medical device MAHs, etc. to further ensure cybersecurity of medical devices, points to consider for the management of vulnerabilities, etc. are summarized as follows. Please disseminate the information to the relevant MAHs, etc. under your jurisdiction and give instructions, etc. to secure the systems.

Please note that a copy of this notification will be sent to the Chief Executive of the Pharmaceuticals and Medical Devices Agency, the Chairman of the Japan Federation of Medical Devices Associations, the Chairperson of the American Medical Devices and Diagnostics Manufacturers' Association, the Chair of the EBC Medical Equipment and Diagnostics Committee, the President of the Japan Association of Clinical Reagents Industries, and the Representative Organizer of the Association of Registered Certification Bodies under PMD Act.

1. Management of vulnerabilities

Vulnerabilities are defects or weaknesses in the design, introduction, or operational control of a system. They may be exploited to breach the security policy of the system (JIS T 81001-1:2022 3.4.22). Therefore, in order to

ensure the cybersecurity of medical devices, medical device MAHs, etc. should identify, evaluate, disclose, and correct vulnerabilities of the medical devices. The following should be considered for the management of these vulnerabilities:

(1) In order to identify and detect vulnerabilities, medical device MAHs, etc. should cooperate with the medical institutions, etc. and make efforts to collect information from the websites of the Information-technology Promotion Agency, Japan (IPA) and the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) in a timely manner. For the collection of the information in a timely manner from the website of the IPA or JPCERT/CC, it is necessary to register the e-mail address to the information service office in IPA or JPCERT/CC. However, this does not apply to the case where the necessary information is collected pursuant to the provision of Article 7 of the Ministerial Ordinance on Good Vigilance Practice for Drugs, Quasi-drugs, Cosmetics, and Medical Devices (MHLW Ordinance No. 135 of 2004).

<IPA>
Register your email address by referring to the following website.
Reference: https://www.ipa.go.jp/mailnews.html (only in Japanese)

<JPCERT/CC>
Send an e-mail to announce-join@jpcert.or.jp with the blank subject and text.
Reference: https://www.jpcert.or.jp/announce.html (only in Japanese)

(2) When the medical device MAHs, etc. obtain information that is considered to be related to a vulnerability of their own product, they should establish procedures to receive, confirm, and evaluate the information, and to implement correction measures, mitigation measures, or supplementary measures based on the information. In addition, they should also establish procedures to provide information to the medical institutions that use the relevant product on how to deal with the vulnerability related to their product, including supplementary measures.

(3) When the medical device MAHs, etc. have confirmed a vulnerability related to their own product, they should take action in accordance with the procedures described in the Information Security Early Warning Partnership. In addition, they should disclose the information in a timely

manner within an appropriate range in consideration of the impact on other medical device MAHs, etc., not just disclosing in-house correction measures, mitigation measures, or supplementary measures.

<IPA>
See the following website and handle information related to vulnerabilities based on “5. Response of Product Developers” in the Information Security Early Warning Partnership Guideline 2019 rev.2.
Reference:https://www.ipa.go.jp/security/guide/vuln/partnership_guide.html
(only in Japanese)

In the Information Security Early Warning Partnership, the IPA is a reception organization for the notification of vulnerability-related information, and the JPCERT/CC, the coordinating organization, will contact medical device MAHs and make arrangements to disclose it.

(4) Concerning 1. (1) to (3) above, if there are any questions about the contents of actions to be taken by medical device MAHs, etc., refer to the FAQ on the IPA or JPCERT/CC website, and if necessary, consult the IPA or JPCERT/CC to establish a system that enables a series of the appropriate management of vulnerabilities and to take appropriate actions on a daily basis.

<IPA>
vuln-inq@ipa.go.jp
Reference:https://www.ipa.go.jp/security/todokede/vuln/uketsuke.html
(only in Japanese)

<JPCERT/CC>
vultures@jpcert.or.jp
Reference: https://www.jpcert.or.jp/reference.html (only in Japanese)

2. Responding to cyber attacks

It is necessary for medical device MAHs, etc. to design and develop medical devices so that their resistance to cyber-attacks can be secured, and to ensure proper operation of medical devices in the intended use environment, information sharing, management of vulnerabilities, etc. after marketing. In response to these cyber-attacks, pay attention to the following points:

(1) In order to prepare the system in advance for the cases (including suspected cases) where medical institutions, etc. are under cyber-attacks, medical device MAHs, etc. should provide medical institutions, etc. with the necessary information on medical devices to be marketed and update the information in a timely manner.

(2) The medical device MAHs, etc. should deliver medical devices to medical institutions after explaining the cybersecurity maintenance plan and policies and roles for handling incidents.

(3) If a medical institution is under a cyber-attack related to a medical device, the medical device MAHs, etc. should cooperate with the medical institution based on the contents of information organized in advance and cooperate for the restoration of medical provision.

(4) Regarding the contents of the 2. (3) above, please note that you can consult with the Information Security Consultation Desk provided by the IPA or JPCERT/CC, if necessary.

<IPA>
anshin@ipa.go.jp
Reference: https://www.ipa.go.jp/security/anshin/about.html (only in Japanese)

<JPCERT/CC>
Please refer to the following website:
Reference: https://www.jpcert.or.jp/form/#report (only in Japanese)

3. Other

For information on cybersecurity of medical devices, refer to the following website of the MHLW.
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000179749_00009.html
(only in Japanese)