This English version is intended to be a reference material to provide convenience for users. In the event of inconsistency between the Japanese original and this English translation, the former shall prevail.

PSB/PSD Notification No. 0115-2
January 15, 2024

To: Directors of Prefectural Health Departments (Bureaus)

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

Basic Principles for Adverse Events Reporting Regarding 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, MHLW, dated April 28, 2015) requires appropriate cybersecurity risk management for medical devices to ensure the safe use of medical devices. The specific risk management regarding cybersecurity of medical devices and the principles for cybersecurity measures and actions have been compiled in the “Guidance on Ensuring Cybersecurity of Medical Devices” (PSEHB/MDED Notification No. 0724-1 and PSEHB/PSD Notification No. 0724-1 dated July 24, 2018, 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). According to the guidance, the marketing authorization holder (hereinafter referred to as MAH) must handle malfunctions or adverse events of medical devices associated with cyber risks as the safety management information specified in the “Ministerial Ordinance for Good Vigilance Practice for Drugs, Quasi-drugs, Cosmetics, and Medical Devices” (MHLW Ordinance No. 135 issued in 2004) and practice appropriate post-marketing safety management.

Reporting of malfunctions or adverse events by MAHs, etc. is specified in

This English version is intended to be a reference material to provide convenience for users. In the event of inconsistency between the Japanese original and this English translation, the former shall prevail.

Article 68-10, Paragraph 1 of the Act on Securing Quality, Efficacy and Safety of Products Including Pharmaceuticals and Medical Devices (Act No. 145 of 1960) and the handling of the reporting is explained in the “Partial Amendment of the Reporting of Adverse Drug Reactions, etc.” (PSEHB Notification No. 0730-8 dated July 30, 2021, issued by the Director of Pharmaceutical Safety and Environmental Health Bureau, MHLW).

This time, in order to further ensure cybersecurity of medical devices, the “Basic Principles for Adverse Events Reporting Regarding Cybersecurity of Medical Devices” has been compiled, as shown in the appendix, concerning the reports by MAHs, etc. on malfunctions or adverse events. These basic principles were created by the Cybersecurity Working Group in the “Studies on Post-Marketing Safety Measures for Safer and More Effective Use of New Forms of Medical Devices” (Health, Labour and Welfare Policy Research Grants (Research Projects on Regulatory Science for Pharmaceuticals and Medical Devices), principal investigator: Atsuko Miyajima, Section Chief, Division of Medical Devices, the National Institute of Health Sciences). Please understand the content and inform the relevant MAHs, etc. under your jurisdiction and provide guidance so that their post-marketing safety management of medical devices can be performed smoothly to further ensure cybersecurity of medical devices.

This English version is intended to be a reference material to provide convenience for users. In the event of inconsistency between the Japanese original and this English translation, the former shall prevail.

Appendix

Basic Principles for Adverse Events Reporting Regarding Cybersecurity of Medical Devices

1. Introduction

In recent years, ensuring the cybersecurity (CS) of medical devices has become a major social challenge owing to the acceleration of the IoT (Internet of Things) of medical devices and the construction of intranet environments within hospitals, as well as the sophistication of cyber-attacks. Medical devices are distributed both within and outside Japan, and medical devices connected to the Internet may undergo cyber-attacks beyond the border framework. For the purpose of international harmonization of CS regulations, at the International Medical Device Regulators Forum (IMDRF), the Medical Device Cybersecurity Guidance N60, “Principles and Practices for Medical Device Cybersecurity” (hereinafter referred to as “IMDRF/CYBER WG/N60 Guidance”) was compiled. In Japan, through PSEHB/MDED Notification No. 0513-1 and PSEHB/PSD Notification No. 0513-1 dated May 13, 2020, issued jointly by the Directors of the Medical Device Evaluation Division and the Pharmaceutical Safety Division of the Pharmaceutical Safety and Environmental Health Bureau, Ministry of Health, Labour and Welfare (hereinafter referred to as MHLW), “Publication of Guidance on Principles and Practices for Medical Device Cybersecurity by International Medical Device Regulators Forum (IMDRF) (Request for Dissemination),” it was described that the IMDRF/CYBER WG/N60 Guidance shall be applied to medical device MAHs. In addition, in order to further strengthen measures against cyber-attacks on medical devices and to ensure the safety of medical devices in clinical settings, the development goals and evaluation criteria for the CS of medical devices have been formulated and 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 (hereinafter

referred to as the “Essential Principles”) was revised. Article 12, Paragraph 3 of the revised Essential Principles has been applied since April 1, 2023, and a transitional measure period was set for 1 year.

Basically, for CS of medical devices, it is important to prevent medical device malfunctions and disadvantages to patients from cyber-attacks. In ensuring the medical devices CS, before marketing, medical devices should be designed and developed to ensure their resistance to cyber-attacks. After marketing, it is necessary that proper management, such as the use in the intended environment, correction of vulnerabilities (patches, updates), and handling of incidents, be mutually carried out by the marketing authorization holder (hereinafter referred to as MAH) and the medical institution as a user of the medical device. Even if the CS measures are considered sufficient at that point, it is difficult to deal with unknown vulnerabilities in the future and there exists a possibility that malfunctions, etc. may occur due to cyber-attacks. In addition, it is necessary to consider that malfunctions, etc. caused by cyber-attacks may occur at any time if the response for CS of medical devices and the information provision by MAHs are left unperformed for already-known serious vulnerabilities. For a medical device, if an unaddressed vulnerability is exploited to allow entry, or if the medical device is infected by aggressive malware, not only the device but also other medical devices with similar vulnerabilities and the whole medical system may be impacted. Unlike ordinary malfunctions, the repercussion of the impact could be extremely large. Therefore, it is necessary to take prompt actions specializing in CS. In addition, in order to prevent new damage, it is necessary to promptly investigate the cause and take appropriate safety assurance measures. This document summarizes the basic principles of medical device CS for MAHs under the adverse event reporting system.

2. Scope of this document

This document applies to the medical devices include programmable medical devices (SaMD: Software as a Medical Device) that can be connected to other devices including media, networks, etc. by wireless or wired connection, and the accessories using programs among the medical devices defined in Article 2, Paragraph 4 of “Act on Securing Quality, Efficacy and Safety of Products

Including Pharmaceuticals and Medical Devices" (Act No. 145 of 1960, hereinafter referred to as the "Pharmaceuticals and Medical Devices Act"), which regulates marketing of medical devices.

The purpose of this document is to organize the basic principles for MAHs regarding post-marketing safety measures focusing on the adverse event reporting system for the medical device CS. In addition, this document presents the cases for which the reporting is expected to be required, at present, based on the Pharmaceuticals and Medical Devices Act. For the pre-marketing medical device CS, the Appendix "Guidance for the Introduction of Cybersecurity of Medical Devices" to the "Guidance for Ensuring Cybersecurity of Medical Devices and Thorough Implementation" (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) should be used as a reference. In addition, the IMDRF has compiled additional guidance. Based on this guidance, the "Revision of the Guidance for the Introduction of Cybersecurity of Medical Devices" was issued, and the "Guidance for the Introduction of Cybersecurity of Medical Devices (Version 2)" for medical device MAHs was presented (PSEHB/MDED Notification No. 0331-11 and PSEHB/PSD Notification No. 0331-4, dated March 31, 2023, jointly issued by the Directors of Medical Device Evaluation Division and the Pharmaceutical Safety Division of the Pharmaceutical Safety and Environmental Health Bureau, MHLW).

As for the medical information system of medical institutions, etc., the MHLW issued the "Guidelines for Safety Management of Medical Information System" (Version 1 was presented in March 2005. It was revised as needed according to the situation and Version 6.0 was issued in May 2023; hereinafter referred to as "Safety Management Guidelines"). For the CS of medical devices at medical institutions, under the Research on Regulatory Harmonization and Evaluation of Pharmaceuticals, etc. by the Japan Agency for Medical Research and Development, the results of the "Research on Extraction of Issues Related to Cybersecurity of Medical Devices at Medical Institutions" (Research and Development Representative: Shohei Nakano, Executive Director, Japan

Association for the Advancement of Medical Equipment) were compiled. Then, the Appendix “Guidance for Ensuring Cybersecurity of Medical Devices at Medical Institutions” to “ Guidance for Ensuring Cybersecurity of Medical Devices at Medical Institutions” was issued (HPB/SDMM Notification No. 0331-1, PSEHB/MDED Notification No. 0331-16, PSEHB/PSD Notification No. 0331-8, dated March 31, 2023, jointly issued by the Counselor for Health Policy Bureau, MHLW [Counsellor for Assistance for Development of Specified Drugs and Medical Information Management], Directors of the Pharmaceutical Evaluation Division and the Pharmaceutical Safety Division of the Pharmaceutical Safety and Environmental Health Bureau).

In addition to this document, the “Safety Management Information on Medical Devices, Guidance for Malfunction Reports” (hereinafter referred to as the “Guidance for Malfunction Reports”) compiled by the Japan Federation of Medical Devices Associations and other relevant guidelines in Japan and overseas should also be used as references.

3. Glossary

(1) Malfunctions etc.

The event of “malfunctions” is generally defined as being in a poor condition*. This includes events that occur due to factors on the part of the user, regardless of whether the failures or “malfunctions” of the device are not related to the device itself. The malfunction concerns all medical devices. The same applies to CS. Malfunction events can be classified as follows:

Types of “malfunctions, etc.” of medical devices

- ✓ Specification issue
- ✓ Defective products
- ✓ Failures/damages
- ✓ Inadequate description of instructions for use, etc.
- ✓ Adverse events caused by a medical device

“Malfunctions, etc.” were classified into the 5 types above, but malfunction events are various, ranging from such events where it is necessary to take safety

measures and minimize the impact on others as soon as possible, to minor events that do not require urgent measures or events with known mechanisms of occurrence and frequency. “Adverse events caused by a medical device” may be caused by any of the above 4 types of malfunctions or by other factors.

*: The “impact of a malfunction” refers to the impact of a poor condition broadly such as breakage, faults, etc. regardless of any stage of the design, marketing, distribution, or use of the device. (“Reporting of Adverse Drug Reactions” [PFSB Notification No. 1002-20 dated October 2, 2014, issued by the Director-General of the Pharmaceutical and Food Safety Bureau, MHLW])

(2) Vulnerability

In JIS T 81001-1:2022 3.4.22, “vulnerability” is defined as follows:

“Vulnerabilities” are defects or weaknesses in the design, introduction, or operational control of a system, which may be exploited to breach the security policy of the system.

For medical devices, the use of third-party software is increasing as functions and performance are improved through networks, etc. Therefore, known vulnerabilities as well as unknown vulnerabilities, which are difficult to discover during design verification, must be considered.

In general, if a vulnerability is exploited, “unauthorized change in device settings,” “unauthorized change or invalidation of diagnosis/treatment,” “loss or disclosure of confidential data,” “false operation of device,” “attack/spread to other devices/systems,” etc. are assumed. These could cause various events classified as “(1) malfunctions, etc.” of the medical device.

(3) EOL, EOS, and legacy medical devices

For medical devices, “EOL (End of Life), EOS (End of Support), and legacy medical devices” are defined in the “Guidance for the Introduction of Cybersecurity of Medical Devices (Version 2)” as follows:

EOL (End of Life)	Life cycle stage of a product starting when the manufacturer no longer sells the product beyond their useful life as defined by the manufacturer and the product has gone through a formal EOL process including notification to users. (Source: the IMDRF/CYBER WG/N60 Guidance)
EOS (End of Support)	Life cycle stage of a product starting when the manufacturer terminates all service support activities and service support does not extend beyond this point. (Source: the IMDRF/CYBER WG/N60 Guidance)
Legacy medical devices	Medical devices that cannot be reasonably protected against current cybersecurity threats, such as updates or supplementary measures, against current cybersecurity threats, regardless of the number of years since the launch of the devices. (Partially modified from the Japanese translation of the IMDRF/CYBER WG/N60 Guidance)

4. Adverse event reporting of medical devices by marketing authorization holders

(1) Basic matters for adverse event reporting of medical devices

When an MAH, etc. becomes aware of a case which is suspected to be due to a malfunction of the medical device or becomes aware of a malfunction which may cause serious health hazards in patients, pursuant to the provisions of Article 68-10, Paragraph 1 of the Pharmaceuticals and Medical Devices Act, he/she shall refer to “Partial Amendment of Reporting of Adverse Drug Reactions, etc.” (PSEHB Notification No. 0730-8 dated July 30, 2021, issued by the Director-General of the Pharmaceutical Safety and Environmental Health Bureau, MHLW). Then, he/she shall submit the following reports using the designated forms to the Medical Device Safety Division, Office of Manufacturing Quality and Safety for Medical Devices, Pharmaceuticals and Medical Devices Agency (hereinafter referred to as “PMDA”).

- Form 8: Medical Device Malfunction/Infection Case Report (in Japan/overseas)
- Form 9: Report on Investigation of Changes in the Incidence of Malfunctions Related to Medical Devices
- Form 10: Research Report on Medical Devices/Investigation Report on Actions Taken Overseas such as Discontinuation of Manufacturing, Recall, and Disposal
- Form 11: Periodic Report for Designated Medical Devices
- Form 12: Periodic Report on Unknown, Non-serious Medical Device Malfunctions

The reports on malfunctions, etc. shall be submitted to the PMDA within the reporting time frame. The MAH shall promptly make the initial report to the PMDA by fax, etc. for all the cases of deaths in Japan and all the measures taken to prevent the occurrence or spread of public health hazards, such as the discontinuation of manufacturing, import or marketing of medical devices overseas. Under Article 228-20, Paragraph 2 of the Enforcement Regulations of the Pharmaceuticals and Medical Devices Act, depending on the seriousness of the health hazard that occurred or may occur, it is required to report it to the PMDA as a 15-day or 30-day report from the date of obtainment of the information or as a periodic report.

At the start of the investigation, the investigation activities should always be carried out on the assumption of the strict reporting time frame of 15-day. Even if the investigation of the matter to be reported is not completed within the time frame, the reporting time frame shall be strictly observed. In such a case, the investigation results obtained by that time shall be regarded as an incomplete report, and the level of disability that the patient/user has or may have due to the event that occurred shall be reported to the best of the knowledge of the MAH. It is required to be consistent with the report from the medical institution, but in the case of the initial report in an emergency, its accuracy is not questioned. In such a case, state in the column for future actions in the designated form that an additional report will be made and make the report by the reporting deadline. At a later date, when a follow-up report is submitted, the reporting company should

make efforts to improve the accuracy. The consistency with the report from the medical institution should be considered at that time.

(2) Adverse Event reporting regarding cybersecurity

Reporting malfunctions, etc. related to medical device CS shall also be made pursuant to various laws, regulations, notifications, etc. shown in (1) in the same way as usual reports of malfunctions, etc.

The MAH should evaluate the impact, etc. of the collected information of the vulnerability of the medical device on the efficacy, safety, etc. If the malfunction of the medical device has occurred related to CS and a health hazard has occurred or may occur, or if safety assurance measures for the overseas medical device have been taken against the vulnerability, it is necessary to examine the necessity of reporting malfunctions, etc.

The case examples of possible medical device malfunctions that may occur in association with the CS and that are to be reported are shown below. At present, since there is little accumulation of malfunction cases related to CS, MAHs should not use the case examples alone as materials for judgment but should give full consideration to the situation of use and (potential) health hazards, etc. It is necessary to determine the necessity of reporting appropriately pursuant to Article 228-20, Paragraph 2 of the Enforcement Regulations of the Pharmaceuticals and Medical Devices Act. The case examples shown below were discussed as malfunctions of CS by the Cybersecurity Malfunction Reporting Sub-WG under the WG of the Revision of Guidance for Malfunction Reporting of the PMS Committee of the Japan Federation of Medical Devices Associations (hereinafter referred to as “JFMDA”). In addition to this document, refer to the revised version of the Guidance for Malfunction Reports. For events that occurred in legacy medical devices, the necessity of reporting malfunctions, etc. should be considered similarly.

Case examples common to all medical devices

- A vulnerability was recognized, and an exploitation experience (false operation, dysfunction, etc.) occurred due to unauthorized access*.

- The failure to apply pre-planned upgrade options (i.e. improperly left) and the unauthorized access to a vulnerability of the networked legacy medical devices resulted in an exploitation experience (e.g. false operation, dysfunction, etc.).
- Due to a DDoS attack (Distributed Denial of Service attack), the functioning of diagnostic imaging devices, etc. stopped unintentionally.

Case examples of individual medical devices

- The setting was changed due to unauthorized access to an unused network port of the networked infusion pump, resulting in excessive infusion or unintended discontinuation of infusion.
- The setting of the insulin pump was changed due to unauthorized access, and the insulin dose was increased to an unexpected dose, resulting in hypoglycemia.
- The setting of the implantable defibrillator was changed due to unauthorized access, and pacing failure or sensing failure occurred, which induced continuous cardiac arrest and arrhythmia.

*: The MAH has the obligation to collect information (Article 68-2-6, Paragraph 1 of the Pharmaceuticals and Medical Devices Act) and the obligation to report to the government (Article 68-10, Paragraph 1 of the Pharmaceuticals and Medical Devices Act) on the malfunctions that occur throughout the product life cycle of medical devices, including the cases not only up to EOS but also after EOS. For this reason, the MAH needs to appropriately judge the necessity of reporting malfunctions, etc. regardless of whether the exploitation experience due to the unauthorized access occurs before or after EOS.

As described in Article 68-9, Paragraph 1 of the Pharmaceuticals and Medical Devices Act, in the safety management system for the medical device CS, it is important for MAHs, etc. to take appropriate measures when a malfunction occurs in the medical device. Furthermore, it is also important to collect information in a timely and proactive manner under the usual safety management system. After

scientific analysis and evaluation, it is also important to take necessary measures such as promptly providing necessary information to medical institutions, etc. to prevent the expansion of damage. In addition, it is necessary to establish the subsequent CS implementation system by investigating the cause of occurrence and performing self-verification. Safety assurance measures include the following measures:

- Provision of information to medical institutions
- Recall, repair, etc.
- Revision of the package inserts
- Handling of the same product (discontinuation of marketing, discontinuation of manufacturing, disposal, etc.)

All the above operations may be performed redundantly. For the implementation of measures, it is necessary to record them appropriately. In implementing the measures, it is necessary to consider not only reporting them to prefectural governments, the MHLW, and the PMDA, but also reporting them to and sharing information with the relevant parties, including the communication with medical institutions and patients. When preparing urgent safety information, etc. ((Dear Healthcare Professional Letters of Emergent Safety Communication (Yellow Letter), Dear Healthcare Letters of Rapid Safety Communications (Blue Letter)) as safety assurance measures, refer to PFSB/SD Notification No. 1031-1 dated October 31, 2014, issued by the Director of the Safety Division, Pharmaceutical and Food Safety Bureau, MHLW “Guidelines for Provision of Urgent Safety Information, etc.”

On the other hand, when an MAH discloses vulnerability information on their own medical devices, vulnerability information related to other companies’ medical devices, or security advisory, if it is disclosed in a situation where mitigation or supplementary measures have not been drawn up, it may immediately become a target for cyber-attacks. Therefore, the timing of disclosure of the vulnerability information should be well considered. If the impact of the vulnerability is large and general, in addition to their company's measures, in some cases, collaboration beyond fields may be required. In this case, the

MAH, in cooperation with regulatory authorities, etc., should establish and implement a Coordinated Vulnerability Disclosure (CVD) process for conducting the necessary coordination.

(3) Response regarding vulnerability

Not all vulnerabilities are subject to reporting. It is useful to adopt a widely used vulnerability scoring system, such as the Common Vulnerability Scoring System (CVSS) to ensure transparency and conduct analysis and evaluation. However, the CVSS scores (basic value, current value) intended to be used in general information security need to be reevaluated by replacing them with the level of impact on the clinical environment and patient safety as medical devices. One of the reference materials is a guidance for medical devices developed by MITRE Corporation (MITRE Rubric for Applying CVSS to Medical Devices).

For the vulnerability, the MAH shall, based on the Software Bill of Materials (SBOM) and design information, etc. for the medical device, investigate the presence of software where the vulnerability exists and whether or not it has been used, and assess the impact on functional performance, etc. As a result of the comprehensive assessment of intended use, site of use, probability, etc., if death or serious health hazard occurs or is likely to occur due to the exploitation of the vulnerability, the MAH should evaluate and determine the necessity of reporting and the classification of the report, and should report the malfunctions, etc. to the regulatory authorities under the provisions of Article 68-10, Paragraph 1 of the Pharmaceuticals and Medical Devices Act. As a result of the above evaluation, if the medical device is equipped with software that has no vulnerabilities, or if it can be judged that, by taking measures (e.g. security patches), the problem can be removed or the risk can be reduced to a degree that the functional performance is not affected, and therefore there is no risk of health hazard, the MAH is not required to report the malfunctions, etc. to the regulatory authorities. However, monitoring should be performed sequentially, and reporting should be made if it becomes necessary.

(4) Handling of legacy medical devices

In considering the CS of medical devices, it is necessary to take into account the product life cycle of medical devices, the responsibilities of MAHs, and their information provision. Even in the case where the product is designed to have measures against known vulnerabilities, etc., the product may become a legacy medical device immediately even before the EOL, if it is going to be used continuously after EOS when the security update cannot be provided any longer or if an event occurs due to a new urgent vulnerability. The MAH has the obligation to collect information (Article 68-2-6, Paragraph 1 of the Pharmaceuticals and Medical Devices Act) and the obligation to report it to the government (Article 68-10, Paragraph 1 of the Pharmaceuticals and Medical Devices Act) on the malfunctions that occur throughout the product life cycle of medical devices, including the cases not only up to EOS but also after EOS. The continued use of a medical device after its EOS can never be recommended, and it must be understood by all the relevant parties that the medical institution is responsible for the continued use. Therefore, it is important for MAHs to proactively provide information, cooperate with customers, and share their recognition with medical institutions.

5. Information sharing system

Information about malfunctions, etc. of medical devices is shared with the PMDA in the medical device adverse event reporting system under the Pharmaceuticals and Medical Devices Act. As safety measures for the CS of medical devices in Japan, if any malfunction or health hazard occurs related to the CS of a medical device, the MAH shall evaluate the impact, etc. of the medical device, determine the necessity of reporting malfunctions, etc., and report them to the PMDA if necessary. At that time, the MAH is required to share the necessary information with medical institutions, users, regulatory authorities, vulnerability finders, etc., and implement a collaborative approach. That's why the MAH needs to establish and maintain an information sharing system for the collection, evaluation, and reporting of information on vulnerabilities. In addition, continuous development of human resources is also desired.

In Japan, regarding the CS, the Cabinet Office, the Ministry of Economy, Trade and Industry, the National Police Agency, and other independent administrative

agencies and private non-profit organizations actively collect and provide information to related companies, etc. The MHLW, having jurisdiction over the adverse event reporting of medical devices, also provides information about vulnerabilities to MAHs and other healthcare professionals pursuant to the Administrative Notice, “Cyber Attacks by Ransomware Targeting Medical Institutions (Alert)” dated June 28, 2021.

6. Summary and future prospects

In this document, as safety measures for the CS of medical devices in Japan, the principles for matters to be reported were organized for cases where a medical device malfunction or health hazard occurs related to CS or any malfunction that may cause serious health hazards to patients is found.

Considering various efforts overseas, in the future, it is desired that a specific procedure to share information among the relevant parties be established and the information be dealt with in cooperation in cases where information on the CS of medical devices is obtained.