

Cybersecurity Requirements for Internet-of-Medical-Things (IoMT) Medical Devices

Effective Date: 01 January 2027 | Issued: 04 August 2026

1. Purpose and Scope

This guidance applies to all medical devices that communicate via wired or wireless interfaces including Bluetooth Low Energy (BLE), Wi-Fi (802.11 series), cellular (4G/5G), Near Field Communication (NFC), and USB. It establishes pre-market documentation requirements and post-market monitoring obligations for manufacturers seeking product approval from MFDS for IoMT medical devices.

2. Device Category Definitions

Category A — Standalone Connected Devices: Medical devices that communicate independently without dependency on a hospital network or cloud infrastructure for core clinical functionality. Examples include Bluetooth-enabled blood glucose meters and Wi-Fi-enabled pulse oximeters.

Category B — Network-Integrated Systems: Devices that form part of a hospital information system or device network where clinical functionality depends on network availability. Examples include networked patient monitoring systems and PACS-integrated imaging devices.

Category C — Cloud-Dependent Devices: Devices where core clinical functionality relies on cloud processing, including AI-assisted diagnostic devices with server-side inference engines.

3. Software Bill of Materials Requirements

Manufacturers must submit a complete Software Bill of Materials (SBOM) in machine-readable format. Accepted formats are CycloneDX version 1.4 or later, and SPDX version 2.3 or later. The SBOM must enumerate:

- All first-party software components at version level
- All third-party components including open-source libraries, with SPDX licence identifiers
- All Software of Unknown Provenance (SOUP) items with risk classification
- Cryptographic algorithms and key management mechanisms

4. Vulnerability Disclosure Timelines

Severity	CVSS Score Range	Disclosure Deadline
Critical	9.0 – 10.0	30 days from confirmed identification

High	7.0 – 8.9	60 days from confirmed identification
Medium	4.0 – 6.9	90 days from confirmed identification
Low	0.1 – 3.9	90 days from confirmed identification

5. International Alignment

This guidance is developed in alignment with IEC 81001-5-1:2021 (Health software and health IT systems safety, effectiveness and security), the IMDRF Principles and Practices for Medical Device Cybersecurity (N60 Final), and the US FDA Cybersecurity in Medical Devices Guidance (September 2023). MFDS will participate in IMDRF cybersecurity working group sessions to ensure continued international harmonisation.