

# Japan PMDA Medical Device Cybersecurity Guide

Reviewed 2026-10-18 | Prepare Japan-specific cybersecurity evidence: MHLW essential principles, JIS T 81001-5-1, local responsibilities, and adaptation of existing device records.

Japan requires relevant medical devices to meet the cybersecurity provisions of Essential Principles Article 12(3). Conformity has been required after the one-year transition ended on April 1, 2024. The implementation approach uses JIS T 81001-5-1:2023 and additional MHLW conformity requirements. Prepare controlled evidence for the device, released software, operating environment, and lifecycle, with local regulatory responsibilities defined.

[Download the matching Japan cybersecurity PDF.](#)

This guide is for product security, engineering, and RA/QA teams preparing a Japanese market entry or maintaining an existing product. [MDC Crosswalk](#) is a companion multi-market planning resource. The PMDA and MHLW sources below are the authorities for Japanese requirements. Japanese originals prevail over reference translations.

## Legal requirement versus implementation material

MHLW Notification No. 67 amended the Essential Principles with Article 12(3). PMDA's [official cybersecurity register](#) explains the April 1, 2023 effective date and one-year transition. This is not simply voluntary adoption of international guidance.

Distinguish the binding Essential Principles from administrative notifications, Q&As, and explanatory material. The latter explain the regulator's conformity expectations; they are not all separate statutes. The applicable approval, certification, or notification pathway depends on the product. PMDA is not necessarily the reviewer for every device pathway.

## Applicability: do not stop at internet connectivity

The provision concerns software-using medical devices connected to other devices or networks, or exposed to foreseeable unauthorized access or attack. The [January 2024 Q&A](#), Q1, includes maintenance-only connections and cloud-accessed medical device software.

Record these decisions:

- Does the product use software, and what is the regulated device boundary?
- Which interfaces connect during clinical use, installation, servicing, updates, or maintenance?
- Can a foreseeable access or attack path affect safety or performance even without continuous internet access?
- Which marketed configurations, companion applications, and services support intended operation?
- Which evidence and local regulatory pathway apply to that product?

A disconnected treatment mode is not, by itself, an exemption. Keep the applicability rationale controlled and review it when interfaces or workflows change.

## JIS T 81001-5-1 and additional conformity items

Japan's implementation materials reference JIS T 81001-5-1:2023. The [July 2023 Q&A](#), Q1, explains that the conformity notification also contains items not explicitly within JIS, including security-contact arrangements and customer vulnerability-disclosure procedures.

Use the licensed Japanese standard and the current notifications for a formal assessment. An IEC checklist or certificate alone does not establish complete conformity with the Japanese Essential Principles. Our [IEC security lifecycle evidence table](#) is a planning aid, not a substitute for the JIS text or Japanese requirements.

## Evidence adaptation table

The artifact examples below are practical working records. Their names are not a universal list of mandatory application attachments.

| Evidence area                     | Japan-specific adaptation                                                                                      | Manufacturer responsibility                                              |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| Product boundary and architecture | Document Article 12(3) applicability, service interfaces, cloud dependencies, and marketed configurations      | Engineering / RA/QA agree the scope and pathway                          |
| Security lifecycle                | Map controlled procedures and evidence to JIS and additional conformity-notification items                     | Engineering and QA maintain procedures and approvals                     |
| Threat and security risk analysis | Link threats, controls, testing, residual risk, and safety consequences where relevant                         | Product security prepares evidence; authorized manufacturer accepts risk |
| Component inventory / SBOM        | Identify the controlled SBOM reference, required coverage/fields, maintenance, and availability                | Configuration management keeps released-build records current            |
| Security test results             | Demonstrate mitigation implementation/effectiveness and retain scope, configuration, findings, and disposition | Engineering / product security retain evidence and retests               |
| Vulnerability handling            | Define security contact, customer communication, triage, remediation, and local reporting assessment           | Product security and Japanese regulatory functions coordinate response   |
| User and environment information  | Adapt supported configuration, installation, update, and compensating-control instructions for local use       | Manufacturer approves local information and responsibilities             |

Reuse accurate architecture, threat, test, and component records from other markets when the product/build matches. Reassess references, scope, labeling, local communication, and application placement. Do not claim a fixed percentage is reusable or that translation alone establishes Japanese conformity.

## **SBOM: maintain it and identify it correctly**

The July 2023 Q&A, Q5-6, explains that SBOM creation should be identified in relevant approval/certification applications and the SBOM must be available for presentation, but routine submission of the SBOM itself is not necessary. It is not simply optional evidence.

Q6 describes component coverage and seven information elements: supplier, component name, version, other unique identifiers, dependency relationships, author of the SBOM data, and timestamp. Check the current source and the applicable application's instructions before choosing fields or attachments. Keep the inventory tied to released software and use it in vulnerability management, not only at application time.

## **Existing products and Annex F**

The July 2023 Q&A, Q2, addresses products already marketed and continuing to be manufactured or marketed after April 1, 2024: maintain identifiable internal records covering conformity-notification requirements. Do not assume blanket grandfathering.

For eligible existing approved, certified, or notified products not developed under JIS T 81001-5-1, Q3 describes use of Annex F for transitional health software. Risk assessment, updated security operating guidance, compensating controls, and partial rewriting may be relevant. The manufacturer must establish the required risk acceptability and identify Annex F use in applicable application materials.

Annex F is not another calendar extension or a way to avoid cybersecurity responsibilities. Evaluate its actual provisions and applicability using the licensed standard and official Q&A, and retain the assessment and manufacturer approval.

## **Security testing and vulnerability response**

Q7 of the July 2023 Q&A says third-party testing is not inherently mandatory when implementation and effectiveness of threat mitigations can be demonstrated. Choose appropriate security testing and independence for the product's risks and evidence needs. A generic network report does not demonstrate every device control.

For postmarket work, connect vulnerability intake to device/build identification, exploitability assessment, relevant clinical consequences, manufacturer action decisions, and Japanese regulatory reporting assessment. The [March 2024 vulnerability-management notification](#) provides an English reference translation; the Japanese original controls. Do not assume every CVE is a reportable adverse event or borrow a different country's reporting clock.

## Worked adaptation example

This is fictional. A manufacturer has an FDA-oriented cybersecurity file for a connected monitoring device and plans a Japanese configuration with a local service partner.

| Existing record                                    | Required review before reuse                                                                                               |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| Threat model for a remote service interface        | Confirm the Japanese service workflow, access roles, connection method, and attack paths are covered                       |
| Release-specific SBOM and vulnerability assessment | Confirm component coverage and Q&A fields; identify the controlled record and its availability in the relevant application |
| Security test report                               | Check the marketed build and environment, local interface changes, findings, remediation, and effectiveness evidence       |
| US vulnerability-management plan                   | Add local contact/customer communication and Japanese reporting decisions; do not replace them with FDA references         |
| Secure lifecycle procedures                        | Map to JIS and additional conformity items; document any justified transitional-software approach                          |

The example is not an approval claim. The manufacturer and its local regulatory partners determine the actual pathway and application content.

## Readiness checklist

- Establish Article 12(3) applicability and product boundaries.
- Identify the Japanese pathway and responsible local regulatory parties.
- Map lifecycle evidence to JIS plus additional notification requirements.
- Keep the released-build SBOM and vulnerability analysis available and controlled.
- Verify threat-to-control-to-test traceability and manufacturer risk approval.
- Evaluate Annex F only where applicable; retain the rationale.
- Align local operating information, security contacts, and customer communication.
- Integrate ongoing vulnerability handling and Japanese reporting assessment.

## How Blue Goat Cyber helps

We support threat modeling, security risk assessment, SBOMs, penetration testing, and cybersecurity evidence adaptation. Japanese applications, QMS approvals, labeling, regulatory reporting, and risk acceptance remain manufacturer responsibilities with the appropriate local regulatory support. [Book a discovery call](#) to scope the cybersecurity work without a promised regulatory outcome.

## FAQ

### **Are maintenance-only connections outside scope?**

Not automatically. The January 2024 Q&A includes maintenance connections. Assess the actual interfaces and foreseeable access or attack paths.

### **Must every application include the full SBOM file?**

No. The July 2023 Q&A distinguishes identifying its creation and maintaining availability from routine attachment. Confirm the applicable pathway and reviewer instructions.

### **Is independent penetration testing universally mandatory?**

No. The official Q&A permits demonstration of mitigation implementation and effectiveness without an inherent third-party mandate. Select testing and independence appropriate to the product and evidence needs.

### **Does Annex F extend the April 2024 transition?**

No. It is a risk-based transitional-software conformity approach for applicable products, not another grace period.

## Related regional guides

- [EU MDR/IVDR evidence crosswalk](#)
- [UK MHRA cybersecurity guide](#)
- [IEC 81001-5-1 evidence table](#)

## Sources and primary references

- [PMDA: medical device cybersecurity requirements and notification register](#)
- [MHLW: medical device cybersecurity hub](#)
- [March 31, 2023 applicability notification](#)
- [March 31, 2023 manufacturer implementation handbook](#)
- [May 23, 2023 conformity-confirmation notification](#)
- [July 20, 2023 cybersecurity Q&A, including SBOM and testing](#)
- [January 31, 2024 applicability Q&A](#)
- [Cybersecurity malfunction/adverse-event reporting principles](#)
- [March 28, 2024 vulnerability-management notification, English reference translation](#)

Current web guide: <https://bluegoatcyber.com/guides/japan-pmda-medical-device-cybersecurity>

Informational material. Confirm requirements for your device and market. The manufacturer owns risk decisions, QMS approvals, and regulatory submissions. No regulatory outcome is promised.