Turning SBOMs into Real Risk Reduction in Healthcare

Zahra Khani, Principal Product Manager

KEYSIGHT

The Threat Reality: Patient Safety Is the Argument

99%

of hospitals manage at least one device with a known exploited vulnerability

ORDR 2026

$10.9M

avg. US healthcare breach cost, highest of any industry, 14 years running

IBM 2025

6.2

avg. vulnerabilities per medical device, exceeding enterprise hardware

ORDR 2026

60%

of medical devices end-of-life with no available security patches

ORDR 2026

PATIENT HARM IS DOCUMENTED

- 29% of healthcare IT professionals surveyed reported perceived increase in mortality following cyberattacks, Ponemon/Proofpoint 2025
- Ransomware averages 19 days of clinical downtime, delaying surgeries, lab results, medications
- 276 million patient records exposed in 2024, more than double the prior year (HHS portal)

WHY MEDICAL DEVICES ARE THE GAP

- 75%+ of device software is third-party or open-source. The manufacturer owns the risk for all of it
- Software supply-chain attacks increased >200% since 2021
- Without an SBOM, identifying affected devices after a CVE takes weeks, not hours

KEYSIGHT

What Is an SBOM: The Software Ingredient Label

Based on FDA February 3, 2026 guidance and NTIA Minimum Elements

SOFTWARE BILL OF MATERIALS	
Ingredients	
Component Name:	OpenSSL
Version:	3.5.1
Supplier:	OpenSSL Foundation
Unique ID (CPE/PURL):	CPE:2.3:a:openssl… pkg:generic/openssl@3.5.1
Dependencies:	zlib, libssl
Author / Date:	OpenSSL Foundation · 2026-03-01

↑ *Every component — machine-readable*

FDA-Required Fields

NTIA Minimum Elements

Name, version, supplier, unique ID (CPE/PURL), dependency relationships, etc

FDA Additional (Feb 2026)

Software support level, end-of-support date, CISA KEV cross-reference, per-CVE risk documentation

Device Labelling

"Support Life" declaration: the period during which security patches will be provided

✓ CycloneDX / SPDX only

✗ PDF alone = not compliant

KEYSIGHT

Global Obligations: What Actually Applies to Medical Devices

Comon misconception: EU Cyber Resilience Act (CRA) currently EXEMPTS medical devices regulated under MDR/IVDR. Proposed MDR/IVDR revision (Dec 2025) would change this — but it is not yet law.

US United States — FDA §524B + QMSR

Statutory

Machine-readable SBOM required for cyber devices. CISA KEV cross-reference. VEX. CVD (statutory). Support Life label. QMSR Feb 2026 embeds into ISO 13485 QMS.

EU EU MDR/IVDR — GSPR 17 & 18

Evolving

Cybersecurity required in technical documentation now (GSPR 17 & 18). Dec 2025 proposed revision adds explicit SBOM + ENISA reporting via EUDAMED. Still early in the EU's ordinary legislative procedure. Unlikely to enter into force before 2027.

GB UK — MHRA + NCSC

Guidance

New PMS regulations in force June 2025. Serious cyber incidents reported within 15 days (2–10 days for severe threats). No standalone SBOM mandate. Cyber patches require FSCA, with FSNs reviewed by MHRA. SaMD cybersecurity guidance forthcoming.

CA Canada — Health Canada

Guidance

2019 pre-market guidance predates SBOMs. No explicit mandate. IMDRF N73 member, principles inform expectations for connected device submissions.

JP Japan — JIS T 81001-5-1

Required

Mandatory for connected devices since April 2023 (transition ended March 2024). IEC 62304 required for software lifecycle management. SBOM not explicit in PMDA submissions. IMDRF N73 principles guide expectations. Verify with a licensed Japanese MAH.

EU EU NIS2 Directive

Org-level

Applies to manufacturers as organizations, IT/OT security, supply-chain risk. NOT a product SBOM mandate. Hospitals as essential entities must assess supplier cybersecurity. Transposed across most EU member states since 2024.

AU Australia — TGA EP12

Recommended

TGA Nov 2025: manufacturers 'should' maintain an SBOM. Guidance, not mandate. IMDRF N73 signatory. Disclose vulnerabilities to TGA and Australian Cyber Security Centre.

IMDRF N73:2023 — Global Foundation

Foundation

Adopted by FDA, EU MDR, MHRA, PMDA, TGA, Health Canada, Singapore HSA. IMDRF N73 + FDA Feb 2026 guidance covers the majority of global market expectations.

KEYSIGHT

Key Concepts: What These Terms Actually Mean

CVSS — Common Vulnerability Scoring System

A 0–10 score rating severity on paper. Does NOT mean your device is at risk. Exploitability determines that.

e.g. Log4Shell = CVSS 10. But a device that never uses Log4j's network features may not be exploitable at all.

NVD — National Vulnerability Database

US government's comprehensive catalog of all 200,000+ known CVEs with CVSS scores. Most are not actively exploited.

e.g. Every CVE gets published here. It's the starting point for awareness, not the urgency filter.

CISA KEV — Known Exploited Vulnerabilities Catalog

Curated list of vulnerabilities being actively exploited RIGHT NOW. Far smaller than NVD but far higher urgency. FDA recommends cross-referencing your SBOM against this.

e.g. If a component appears on KEV, criminals are already using it today. Act immediately.

VEX — Vulnerability Exploitability eXchange

Manufacturer document stating whether a CVE actually affects their specific device in deployment. Statuses: Not Affected / Affected / Fixed / Under Investigation.

e.g. Reduces hospital alarm fatigue. Tells them which CVEs are real risks in their context.

CVD — Coordinated Vulnerability Disclosure

Formal process to receive, triage, fix, and responsibly disclose vulnerabilities. Mandated by FDA under §524B(b)(1), a statute, not guidance.

e.g. Researcher finds flaw → reports privately → manufacturer fixes → only then disclosed publicly.

SPDF — Secure Product Development Framework

FDA-encouraged framework for building security into every device development stage. Encouraged in guidance as one approach to satisfy QMSR. Other approaches permitted.

e.g. Think of it as a security-focused design lifecycle from threat modelling to post-market patching.

KEYSIGHT

The SBOM Lifecycle: How Manufacturers and Hospitals Connect

1 Manufacturer Generates

- NTIA elements + FDA lifecycle metadata
- Known vulns incl. CISA KEV identified
- CycloneDX or SPDX, machine-readable
- Embedded in ISO 13485 QMS / CI-CD

2 Monitors & Discloses

- Continuous vulnerability + CISA KEV monitoring
- Exploitability assessment per device
- VEX document issued to hospitals
- UK MHRA: 15-day serious incident report

3 Hospital Receives & Acts

- Ingests machine-readable SBOM
- Maps to deployed device instances
- Receives VEX: knows what's exploitable
- Continuous monitoring (not annual)

4 Shared Response

- Manufacturer issues compensating controls
- Hospital applies network segmentation
- SBOM updated; new VEX issued
- Patch after revalidation (6–12 months)

Today: Manufacturers file SBOMs with FDA but rarely share with hospitals. Hospitals receive PDFs they can't act on.

Target: FDA requires manufacturers to continuously share SBOMs with users. NIS2 requires hospitals to assess supplier security.

KEYSIGHT

From CVE to Patient Safety Decision: The 5-Step Process

1

Generate a Complete SBOM

Automated scanning is the starting point. FDA requires completeness. All commercial, open-source, and off-the-shelf components including transitive dependencies. Manual review strongly recommended for legacy devices.

2

Identify All Known Vulnerabilities and Cross-Reference CISA KEV

CISA KEV lists vulnerabilities being actively exploited NOW. FDA guidance recommends this (enforced via deficiency letters). UK MHRA: 15 days for serious incidents. EU MDR proposed revision: ENISA notification required.

3

Assess Exploitability and Issue VEX

High CVSS ≠ exploitable in your device. Assess whether the vulnerable code is reachable in your deployment context. Issue a VEX document: 4 statuses: Not Affected / Affected / Fixed / Under Investigation.

4

Triage by Patient Safety Impact, Not Just CVSS Score

CVSS 9.8 in a non-networked display ≠ CVSS 7.0 in an infusion pump controller. Under QMSR, known vulnerabilities are 'reasonably foreseeable failure modes', same ISO 13485 risk management as any design hazard.

5

Remediate & Disclose: CVD is a Statutory Requirement

CVD is a legal requirement under §524B(b)(1) not guidance. Device revalidation: 6–12 months. Issue compensating controls to hospitals immediately. UK: Field Safety Notice. EU MDR: FSCA. TGA: notify ACSC.

KEYSIGHT

Global Compliance Roadmap: Manufacturers and Hospitals

	MANUFACTURERS
1	Software inventory. Automated scanning + manual gap review. Document unresolvable gaps with formal risk rationale. FDA & IMDRF N73 require completeness.
2	CISA KEV cross-reference + per-CVE documentation. FDA guidance recommends this. Begin VEX drafts for top-risk devices.
3	Integrate SBOM into QMSR/ISO 13485 QMS — design controls (Clause 7.3.7) and CAPA (Clause 8.5). Embed in CI-CD. Required post-Feb 2026.
4	Establish CVD process (statutory, §524B). Define UK MHRA 15-day trigger. Prepare ENISA workflow for future EU MDR obligation.
5	Add Support Life to device labelling. Continuously publish SBOMs to hospital users. EU MDR GSPR requires post-market transparency.

	HOSPITALS
1	Update procurement contracts, require CycloneDX or SPDX + VEX SLAs as contract conditions. EU: directly supports NIS2 supply-chain obligations.
2	Check Support Life label before every purchase. UK NHS NCSC recommends same procurement due diligence.
3	Assign a named SBOM owner across IT security + clinical engineering. NIS2 essential entities require supply-chain risk governance.
4	Ingest SBOMs, Score vendor SBOM quality, Verify their accuracy independently using binary analysis. reject incomplete submissions.
5	Set up continuous CVE + CISA KEV monitoring. Automated alerts, not annual reviews. Map SBOMs to deployed device instances by risk/location.

KEYSIGHT

Common Pitfalls: What Triggers Deficiency Letters and Exposes Patients

MANUFACTURERS

Stale SBOM
Generated at submission only — must be continuously maintained

Incomplete deps
Missing transitive dependencies — where most real CVEs live

PDF only
Does not satisfy FDA's machine-readable requirement; hospitals can't ingest it

No KEV check
CISA KEV cross-reference is FDA-recommended — absence signals gaps

SBOM outside QMS
Post-QMSR Feb 2026: must be ISO 13485 configuration management

No CVD process
Statutorily required under §524B(b)(1) — not guidance language

No Support Life
Recommended in device labelling per FDA June 2025 guidance

Not sharing SBOMs
FDA guidance expects continuous availability to hospital users

HOSPITALS

PDF accepted
Cannot be ingested by tools — false confidence, zero protection

Shared drive
Having the file is not monitoring. Nobody acts when a CVE drops.

Annual reviews
CVEs emerge daily. A KEV hit will not wait for your quarterly cycle.

No VEX SLAs
Without contractual obligation vendors have no incentive to notify promptly

Siloed IT + CE
SBOM data in IT; devices managed by clinical engineering — must share intel

No Support Life
Buying a device expiring mid-service is a documented avoidable risk

No SBOM owner
Diffuse ownership means nobody acts in a crisis

CRA confusion
CRA exempts medical devices — correct framework is NIS2 + MDR

KEYSIGHT

Keysight SBOM Manager

Addressing the Documented Gaps on Both Sides

SBOM Generator

No source code required

- Binary-level extraction from firmware, containers, compiled binaries
- Solves legacy & acquired-codebase completeness challenge
- CycloneDX / SPDX output, machine-readable, FDA-ready
- Addresses: incomplete deps, legacy blind spots

SBOM Studio

For manufacturers

- Continuous CVE + CISA KEV + GitHub Advisories + OSV + EUVD + … monitoring
- VEX document generation and distribution to hospitals
- SBOM quality scoring, auto-correction & NTIA compliance check
- SBOM sharing & distribution · EOL / EOS / component age / operational agility

SBOM Consumer

For hospitals

- Ingests any standard SPDX/CycloneDX formats, quality scoring, auto-correction & NTIA compliance check
- Continuous monitoring, replaces the shared-drive model
- Integrates with existing asset management systems
- Maps SBOMs to deployed devices by group/ward/location

KEYSIGHT

SBOM GENERATOR

Binary analysis: no source code required

THE CHALLENGE

- **75%+** of device software is third-party or open-source
- **Legacy** firmware, original developer long gone, no source
- **Acquired** codebases, no build environment access
- **Hidden** dependencies missed by source-code scanners
- **Shipped** binary ≠ what the build system thinks is there
- **Vendor** SBOMs may be incomplete. Hospitals can't verify without source code either

Next-Gen Binary Detection Engine

Patent-pending technology goes beyond signature matching. Uses binary similarity analysis and code emulation to identify open-source AND closed-source components.

No source code · No build environment · Verify received SBOMs

What It Detects

Firmware images, container layers, compiled binaries, shared libraries. Detects components missed by SCA tools.

Windows · Linux · QNX · containers · VM images · RTOS and monolithic firmware

Output: Machine-Readable SBOM

Produces CycloneDX and SPDX machine-readable SBOMs ready for FDA submission. Output includes full component inventory with dependency relationships, CPE/PURL identifiers, and supplier metadata aligned to NTIA Minimum Elements.

CycloneDX · SPDX · FDA-ready · NTIA-aligned

CVE Reachability Analysis + Automated VEX

Because analysis is binary-level, Generator also determines CVE reachability directly. Identifying the vulnerability reachability, and auto-generating the corresponding VEX statement.

Reachability analysis · Automated VEX

KEYSIGHT

SBOM STUDIO

The manufacturer's operational hub: from component list to patient safety decision

① Continuous Multi-Source Monitoring

Monitors NVD, CISA KEV, GitHub Advisories, OSV, and EPSS simultaneously, not just the NVD. Prioritises authoritative sources over NVD when available, reducing false positives. Daily alert reports with CVSS / EPSS / KEV severity tagging.

② Prioritizing Authoritative Sources

Prioritizes authoritative vulnerability sources over the NVD when available — reducing false positives from NVD's known CPE data gaps. Excludes already-patched vulnerabilities from results entirely, so teams focus only on what is genuinely unresolved.

③ CISA KEV Alerts + Due Date Tracking

Fires immediately when a component enters the KEV catalog. Tracks KEV due dates for each affected product. Configurable alert thresholds by CVSS, EPSS, severity, and KEV status, so your team gets actionable alerts, not noise.

④ SBOM Quality, Auto-Correction & NTIA

Scores each SBOM for completeness and quality. Automatically identifies and corrects SBOM data issues. Checks compliance against NTIA Minimum Required Elements and other regulatory frameworks. Flagging gaps before submission so manufacturers know exactly what is missing and why.

⑤ Secure SBOM Sharing & Distribution

Enables controlled sharing of SBOMs with stakeholders such as hospital customers, regulators, and supply chain partners. Supports FDA expectation that manufacturers make SBOMs continuously available to users.

⑥ Operational Agility

Tracks software support level, end-of-support dates, end-of-life status, component age, and operational agility for every component. Flags components approaching or past their support lifecycle, enabling the Support Life declaration in device labelling and supporting informed risk and procurement decisions.

KEYSIGHT

SBOM CONSUMER

For hospitals: from inconsistent SBOMs to live, ward-level risk intelligence

TODAY, WITHOUT SBOM CONSUMER	WITH SBOM CONSUMER
SBOMs arrive in different formats from different vendors, different tools, sometimes manual creation. Even when labelled SPDX or CycloneDX, many don't fully comply, or are missing fields needed for effective management	✓ Ingests SBOMs in any standard SPDX or CycloneDX format from any vendor and normalises them automatically. No manual conversion, no SBOM expertise required
No way to assess whether a vendor's SBOM is complete or accurate. Missing identifiers create false confidence	✓ Scores each submission for completeness and quality, with specific gap details. 'Your score is 42/100, here's what's missing', giving hospitals concrete leverage in vendor conversations
No way to check whether a vendor's SBOM meets NTIA Minimum Required Elements. Non-compliant submissions get accepted as-is	✓ Checks compliance against NTIA Minimum Required Elements and auto-corrects SBOM data issues where possible
Annual procurement questionnaires are the primary 'monitoring' mechanism. Misses every CVE published between reviews	✓ Continuous automated monitoring runs every day against NVD, CISA KEV, and other feeds. Every deployed device, without manual effort
When a new CVE drops, no automated way to know which deployed devices, down to the ward, floor, or room, are affected. Requires days of manual cross-referencing	✓ Maps every SBOM to specific deployed device instances, group, ward, floor, room. When a vulnerability hits CISA KEV, you know in seconds: the MRI scanner in Suite 4, Floor 3, is affected by this CVE

EU NIS2: Hospitals as essential entities must assess the cybersecurity of their device suppliers. SBOM Consumer is the mechanism. Continuous, evidence-based, documented. No more annual questionnaires.

KEYSIGHT

Key Takeaways: What to Do This Week

MANUFACTURERS — 3 IMMEDIATE ACTIONS

1. Check SBOM completeness: transitive dependencies, all components, CPE/PURL identifiers. Completeness is the foundation everything else depends on.
2. Cross-reference against CISA KEV at cisa.gov/known-exploited-vulnerabilities today. Anything on that list in a deployed product is your most urgent priority.
3. Confirm your CVD process exists. §524B(b)(1) is a statute, not guidance. Named owners, defined timelines, tested notification workflows.

HOSPITALS — 3 IMMEDIATE ACTIONS

1. Update your procurement contract template today. Add CycloneDX or SPDX + VEX update SLAs as contract conditions. Costs nothing. Shifts everything.
2. Assign one named person, not a committee, as SBOM owner across IT security and clinical engineering. Ownership is the most common failure mode.
3. Get your existing SBOMs out of the shared drive and into a vulnerability management workflow. Start by cross-referencing against CISA KEV manually if needed.

See Keysight SBOM Manager in action — two ways to get started today.

Live Product Demo

See binary analysis, continuous monitoring, VEX generation, SBOM quality scoring, and ward-level device mapping working together, on a real device scenario relevant to your portfolio.

Free Proof of Concept

Send us your firmware or software image. Our expert runs Keysight SBOM Manager against your binary, produces a compliance-ready SBOM with full vulnerability intelligence, and walks you through the results.

https://www.keysight.com/be/en/cmp/2026/sbom-manager-proof-of-concept.html