Modernizing Software Supply Chain Risk Management in Healthcare: From Visibility to Action

Ken Zalevsky, CEO & Founder of Vigilant Ops, Inc.

VIGILANTOPS

Introduction

- CEO & Founder of Vigilant Ops, a leading SBOM lifecycle management solution
- 20+ years as Head of Medical Device Cybersecurity at Bayer Healthcare
- Worked with the FDA, U.S. Department of Homeland Security, DITTA, CISA on cybersecurity initiatives

Ken Zalevsky, Vigilant Ops CEO

Email: ken.zalevsky@vigilant-ops.com

VIGILANTOPS

The Healthcare Software Supply Chain

Growing Complexity: Increasing use of third-party and open-source software in medical devices and healthcare IT systems

Regulatory Scrutiny: FDA, HHS, and global regulators now require greater visibility into software components (e.g., Software Bill of Materials (SBOMs))

Cyber Risk Exposure: Software vulnerabilities in connected devices and hospital systems create targets for ransomware and nation-state threats

Shared Responsibility: Security gaps can propagate across vendors, suppliers, and integrators—no single point of failure

Legacy Systems: Older software and devices with unpatchable components remain in clinical use, heightening supply chain risk

Operational Disruption: Compromised software can lead to downtime in critical healthcare services, impacting patient care

Emerging Standards: Initiatives like the Healthcare and Public Health Sector Coordinating Council (HSCC) and NIST are shaping best practices

Call to Action: Need for cross-sector collaboration—manufacturers, providers, and policymakers—to secure the digital supply chain.

Why Healthcare is Especially Vulnerable

High-Value Target: Patient data is lucrative on the black market and vital for care continuity—making it a prime ransomware target

Low Tolerance for Downtime: Cyber incidents can delay surgeries, diagnostics, and treatments—directly impacting patient safety

Widespread Legacy Systems: Many hospitals and clinics run outdated, unsupported software that can't be easily patched

Complex Vendor Ecosystem: Heavy reliance on a fragmented network of third-party software vendors and device manufacturers

Limited Cyber Resources: Many healthcare organizations, especially smaller ones, lack dedicated cybersecurity teams or budgets

Long Device Lifecycles: Medical devices often remain in service for 10–15 years, far outliving modern security standards

Interoperability Demands: Constant pressure to integrate systems (EHRs, imaging, billing) increases attack surfaces

Compliance Over Security: Organizations may prioritize regulatory checkbox compliance over holistic, proactive security strategies

SBOM: Visibility You Can Act On

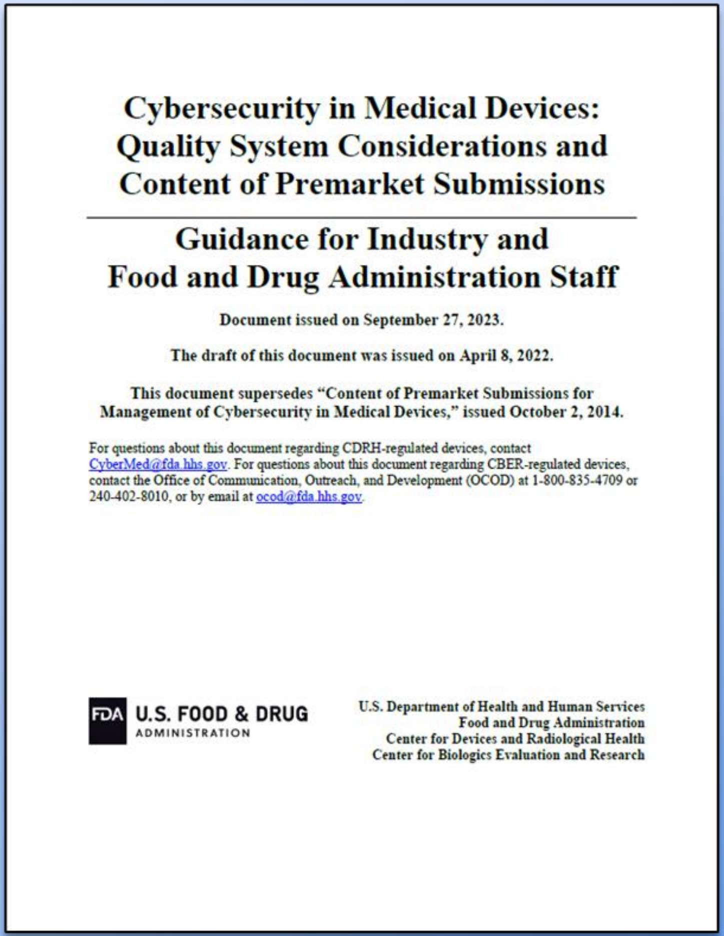
- SBOM Role in Risk Management
- Benefits

SBOM Includes:

- Device (product name)
- Device software component information
    - Name
    - Version
    - Manufacturer
    - Level of support
    - End of support
    - Vulnerabilities
        - Safety and security risk of each vulnerability
        - Controls to mitigate each vulnerability

Regulatory Push: Why The Time Is Now

- FDA premarket guidance requiring SBOMs
- Executive Orders and CISA momentum



Cybersecurity in Medical Devices:
Quality System Considerations and
Content of Premarket Submissions

Guidance for Industry and
Food and Drug Administration Staff

Document issued on September 27, 2023.

The draft of this document was issued on April 8, 2022.

This document supersedes "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," issued October 2, 2014.

For questions about this document regarding CDRH-regulated devices, contact CyberMed@fda.hhs.gov. For questions about this document regarding CBER-regulated devices, contact the Office of Communication, Outreach, and Development (OCOD) at 1-800-835-4709 or 240-402-8010, or by email at ocod@fda.hhs.gov.

FDA U.S. FOOD & DRUG
ADMINISTRATION

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Center for Biologics Evaluation and Research

Real-World Impacts of Poor SBOM Hygiene

Undetected Vulnerabilities: Untracked components allow critical vulnerabilities (e.g., Log4Shell, OpenSSL flaws) to go unnoticed in deployed systems

Delayed Incident Response: Without an accurate SBOM, organizations waste precious time identifying affected systems during a breach

Regulatory Risk: Noncompliance with FDA, EO 14028, and HHS directives can result in warnings, product recalls, or blocked market access

Patient Safety Threats: Vulnerabilities in life-critical devices (e.g., infusion pumps, diagnostic equipment) can lead to clinical harm

Supply Chain Disruption: Lack of SBOM hygiene leads to uncertainty across vendor networks, delaying updates and patches

Reputational Damage: News of preventable cybersecurity incidents erodes patient trust and damages brand credibility

Increased Cost of Ownership: Reactive security efforts, forensic investigations, and legal consequences drive up costs

Barrier to Partnerships: Hospitals and integrators increasingly require SBOM transparency before purchase or integration

Best Practices: Continuous Supply Chain Monitoring

Generate and Share SBOMs: Manufacturers should provide detailed, machine-readable SBOMs; hospitals should request and manage them centrally

Continuously Monitor for Vulnerabilities: Both parties must track known issues (e.g., CVEs, CISA KEVs) using real-time threat intelligence

Automate Detection and Alerts: Implement tools to detect vulnerabilities in software components and alert relevant teams—clinical, IT, or engineering

Track Software Component Lifecycles: Maintain records of component versions and update histories across the product's use and maintenance phases

Assess and Vet Vendors: Hospitals and OEMs should evaluate cybersecurity practices of upstream software suppliers and service providers

Integrate Across Teams: Encourage collaboration between cybersecurity, biomed, regulatory, and procurement teams for coordinated response

Build Incident Response Around SBOMs: Ensure both manufacturers and hospitals can quickly identify impacted systems during a cyber event

Call to Action for Providers

- What healthcare organizations should be asking their vendors today:
  - ✓ Can you provide a machine-readable SBOM?
  - ✓ How do you monitor it post-deployment?

- What healthcare organizations should do internally:
  - ✓ Establish SBOM requirements in procurement
  - ✓ Vet tools and processes to manage SBOMs over time

Q&A

- Questions?
- Feel free to email me at Ken.Zalevsky@vigilant-ops.com

Ken Zalevsky, Vigilant Ops CEO

www.vigilant-ops.com

VIGILANTOPS

Thank You!