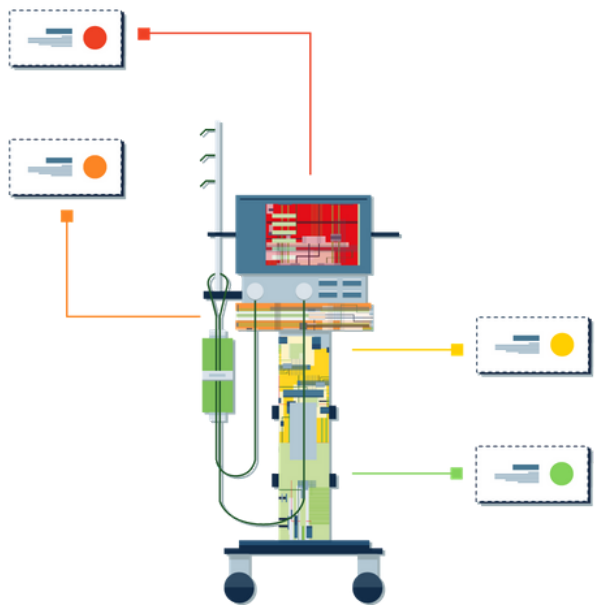
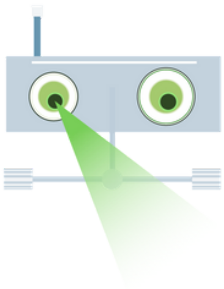
Cynerio

YOUR HANDY SWITCHLIST

MEDICAL DEVICE SECURITY LIFECYCLE MANAGEMENT





Hi, I'm *Switch*!
Use my **Switchlist** - a handy, comprehensive checklist I made to help professionals in healthcare like you manage every stage of the medical device security lifecycle.

Phase 1: Procurement

- [ ] Make a list of all potential stakeholders
  - [ ] Medical Departments
  - [ ] Biomed/CE
  - [ ] IT
  - [ ] Business & Board
- [ ] Check what departments rely on the device

Align your Biomed/CE and IT security teams

- [ ] IT team: confirm your clinical network's capacity can handle more devices
  - [ ] Conduct a risk assessment of the vendor and device model vs. competitors
- [ ] Biomed team: measure departmental/cross-hospital device usage
  - [ ] Measure device efficiency
    Develop ROI profiles
- [ ] Both teams should consult the MDS2 form - does the device comply with your hospital's security policy (e.g. patching strategies, endpoint protection, etc.)?
- [ ] Plan ahead: ensure compliance - assess required compensating controls

Phase 2: Maintenance

Discovery

Secure a 360° view of devices and connections

- [ ] Inventory all devices
  - [ ] Account for every device on the network, per department, per device type
  - [ ] Profile each device
  - [ ] Rate clinical criticality

Cross-Departmental Coordination

- [ ] Conduct cross-organizational, live assessment of current asset inventory
- [ ] Confirm your 360° view of device inventory and connections is consistent across your organization

Scheduling

Ensure scheduled maintenance does not interrupt clinical services

- [ ] Monitor device usage to identify downtime
- [ ] Monitor device criticality

Patch Management

- [ ] Check device MDS2 guidelines and ensure the device has the ability to be patched
- [ ] Make sure the device has the most up-to-date patch available
- [ ] Make sure the device is running the most up-to-date software
- [ ] Make sure the device is running the most up-to-date OS version

Policy Validation

Confirm compliance with organizational policy and official regulations (HIPAA, CDC, FDA, etc.)

- [ ] Ensure live compliance with security policy (e.g. who can log in, identify vendor connections, inter-device communications, etc.)

Segmentation

Coordinate between Biomed/CE and IT teams

- [ ] Plan ahead: ensure new cybersecurity policies will not disrupt connections between critical medical devices
- [ ] IT team: set rules to block unauthorized device communications with VLANs, NACs, and ACLs

Phase 3: Disposal

PHI

- [ ] Identify old devices that store and send PHI
- [ ] Ensure PHI data isn't being leaked
- [ ] Correlate information on PHI between static MDS2 data and live data from the network

Map Connections

Map device connections to ensure:

- [ ] Disconnecting device will not disrupt clinical operations and services
- [ ] Note what other devices connect to this one and how:
  - [ ] Gateway
  - [ ] Cloud services
  - [ ] Local DICOM workstation
  - [ ] Specific ports

Cynerio

About Cynerio

Cynerio is the world's premier medical-first cybersecurity IoT solution. We view cybersecurity as a standard part of patient care and provide healthcare delivery organizations with the insight and tools they need to secure clinical ecosystems and achieve long-term, scalable threat remediation without disrupting operations or the delivery of care.