

Intelas

A Compass One Healthcare
Company

Cybersecurity readiness toolkit for medical devices

Assessing your security posture



Table of Contents:

<u>Introduction</u>	3
<u>Device Inventory and Management</u>	4
<u>Cybersecurity Policies and Procedures</u>	6
<u>Network Security</u>	8
<u>Training and Awareness</u>	10
<u>Monitoring and Incident Detection</u>	12
<u>Vendor Management</u>	14
<u>Backup and Recovery</u>	16
<u>Future Planning and Investments</u>	17



This medical device cybersecurity toolkit is designed to give hospital administrators a comprehensive view of their current cybersecurity practices, policies, and infrastructure related to medical device management. By examining critical areas—such as device inventory, network security, vendor management, and incident response—this questionnaire will help identify vulnerabilities and uncover opportunities to strengthen your hospital’s cybersecurity posture.

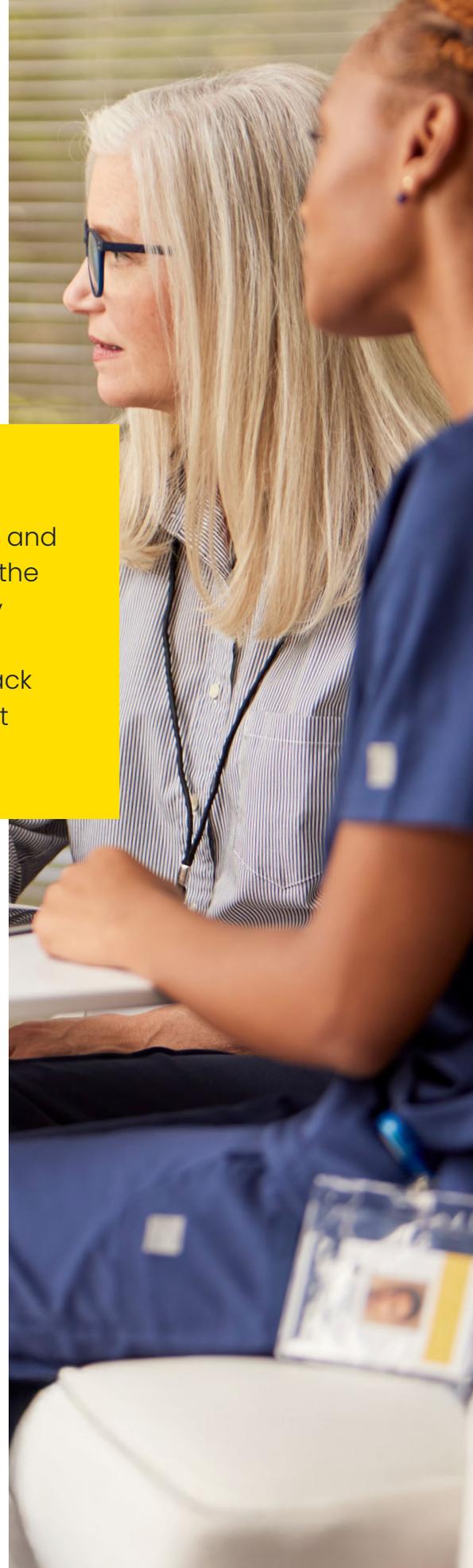
How to use this toolkit:

This tool is intended as both a baseline assessment and a resource for continuous improvement. Complete the questionnaire to evaluate current practices, identify areas needing attention, and prioritize action steps. Use the scorecards and checklists throughout to track your progress and create a tailored action plan that strengthens device security over time.

Completing this assessment will enable your hospital to:

- 1. Enhance patient safety:** Safeguard medical devices against cyber threats that could impact patient care and safety.
- 2. Strengthen cybersecurity posture:** Evaluate and reinforce your cybersecurity framework to defend against evolving threats.
- 3. Ensure compliance:** Align with essential regulatory standards and guidelines, including HIPAA and FDA requirements.
- 4. Optimize resource allocation:** Pinpoint where additional resources or investments are needed to enhance medical device security.
- 5. Facilitate continuous improvement:** Set a baseline for current practices and track progress to drive ongoing cybersecurity advancements.

With a thorough understanding of your hospital’s cybersecurity needs, you can better protect patient data, ensure the reliability of healthcare operations, and foster trust among patients and stakeholders.



Device inventory & management

1. Inventory tracking:

Why it matters: Classifying devices based on criticality and data sensitivity allows for focused security measures where they're needed most.

Best practice: Prioritize critical devices in the cybersecurity strategy, particularly those impacting patient care or handling sensitive data.

Questions to ask:

- Do you maintain a comprehensive inventory of all medical devices connected to the network?
- How often is this inventory updated?
- What system or software do you use to manage the inventory?

Inventory tracking checklist:

- All medical devices inventoried and documented.
- System or software in place to automatically update inventory changes.
- Inventory reviewed at least quarterly.

2. Device classification:

Why it matters: Classifying devices based on criticality and data sensitivity allows for focused security measures where they're needed most.

Best practice: Prioritize critical devices in the cybersecurity strategy, particularly those impacting patient care or handling sensitive data.

Questions to ask:

- Are medical devices classified based on their criticality and impact on patient care?
- Is there a prioritization for devices that handle sensitive patient data?

Device classification checklist:

- Critical devices identified and classified.
- Devices handling sensitive data are prioritized.
- Classification reviewed during cybersecurity audits.

3. Lifecycle management:

Why it matters: The lifecycle management process ensures that every device, from acquisition to decommissioning, remains secure throughout its use.

Best practice: Develop a lifecycle management plan that includes secure disposal and repurposing processes.

Questions to ask:

- How do you manage the lifecycle of medical devices from acquisition to decommissioning?
- Is there a process for securely disposing of or repurposing medical devices?

Lifecycle management checklist:

- A formal lifecycle management plan is in place for all medical devices.
- Secure protocols are established for the acquisition, maintenance, and decommissioning of devices.
- Processes for secure disposal or repurposing of devices are documented and followed.
- Regular reviews are conducted to ensure lifecycle procedures are up-to-date and effective.

Device inventory & management scorecard:

- Inventory completeness: __/5
Evaluate if all connected medical devices are accurately tracked and documented.
- Device classification: __/5
Assess the classification of devices based on criticality and data sensitivity, ensuring prioritized security measures.
- Lifecycle security: __/5
Review the effectiveness of lifecycle management, including secure disposal and repurposing of devices.



Cybersecurity policies and procedures

1. Policy framework:

Why it matters: Policies set the standards for device security and guide staff in handling cybersecurity threats.

Best practice: Review and update policies annually to adapt to new threats and regulatory changes.

Questions to ask:

- Do you have a formal cybersecurity policy specific to medical devices?
- How often is this policy reviewed and updated?

Policy framework checklist:

- Formal policy is in place for medical device cybersecurity.
- Policies reviewed annually.
- All staff trained on updated policies.

2. Compliance:

Why it matters: Compliance with standards like HIPAA and FDA guidelines helps prevent legal issues and maintains patient trust.

Best practice: Regular audits ensure ongoing adherence to all regulatory requirements.

Questions to ask:

- Are your cybersecurity policies aligned with relevant regulations and standards (e.g., HIPAA, FDA guidelines)?
- How do you ensure ongoing compliance with these standards?

Compliance checklist:

- Policies aligned with regulatory standards.
- Annual audits performed.
- Compliance team assigned to oversee adherence.

3. Incident response:

Why it matters: An effective response plan ensures quick action, minimizing disruption and protecting sensitive data.

Best practice: Conduct regular incident response drills to keep staff prepared.

Questions to ask:

- Do you have an incident response plan for medical device cybersecurity incidents?
- How often are incident response drills conducted?

Incident response checklist:

- A documented incident response plan exists specifically for medical device cybersecurity.
- Incident response plan includes clear steps for identification, containment, eradication, recovery, and post-incident review.
- Regular incident response drills are conducted (e.g., quarterly or semi-annually).
- Incident response plan is reviewed and updated annually.
- Designated team members are assigned specific roles in the event of a cybersecurity incident.
- Communication protocols are established for notifying relevant stakeholders during an incident.

Cybersecurity policies and procedures scorecard:

- Policy completeness: __/5
Assess the thoroughness of the cybersecurity policy, specifically addressing medical device security.
- Compliance alignment: __/5
Evaluate the policy's alignment with relevant regulatory standards (e.g., HIPAA, FDA guidelines) and its regular updates to maintain compliance.
- Incident preparedness: __/5
Review the readiness and clarity of the incident response plan, including frequency of drills and team preparedness.



Network security

1. Network segmentation:

Why it matters: Separating medical devices from other IT systems isolates them from broader threats.

Best practice: Monitor and control network traffic between segments to ensure data flow is secure.

Questions to ask:

- Are medical devices on a separate network segment from other IT systems?
- How is network traffic monitored and controlled between these segments?

Network checklist:

- Medical devices on dedicated network.
- Traffic monitoring system in place.
- Access control policies enforced.

2. Access controls:

Why it matters: Limiting access prevents unauthorized users from compromising devices.

Best practice: Implement multi-factor authentication (MFA) where possible.

Questions to ask:

- What authentication mechanisms are in place for accessing medical devices?
- How are user access levels determined and managed?

Access control checklist:

- MFA enabled for high-risk devices.
- Access roles reviewed quarterly.
- User training on secure access procedures.

3. Encryption:

Why it matters: Encrypting data protects it during transmission and at rest, securing patient information.

Best practice: Use end-to-end encryption for all sensitive data.

Questions to ask:

- Is data transmitted from medical devices encrypted?
- Are there protocols for encrypting data at rest on medical devices?

Encryption checklist:

- Encryption is enabled for all sensitive data transmitted from medical devices.
- Protocols are in place for encrypting data at rest on medical devices.
- Annual reviews are conducted to assess and update encryption protocols.
- Encryption practices comply with relevant standards and regulations (e.g., HIPAA, FDA guidelines).
- End-to-end encryption is applied to critical devices and sensitive data.
- Encryption keys are securely managed and stored.

Network security scorecard:

- Network segmentation completeness: __/5
Evaluate if medical devices are isolated from other IT systems and if network traffic is properly monitored.
- Access control effectiveness: __/5
Assess the implementation of multi-factor authentication, access role reviews, and user training on secure access.
- Encryption coverage: __/5
Review the extent of data encryption during transmission and at rest, as well as compliance with regulatory standards.



Training and awareness

1. Staff training:

Why it matters: Consistent training keeps staff up-to-date on best practices and emerging cybersecurity threats.

Best practice: Implement training specific to medical devices, covering access control, incident reporting, and secure handling.

Questions to ask:

- Do you provide regular cybersecurity training specific to medical devices for your staff?
- How do you measure the effectiveness of this training?

Training checklist:

- Regular medical device cybersecurity training provided.
- Training effectiveness measured annually.
- Staff retraining every six months.

2. Awareness programs:

Why it matters: Ongoing awareness keeps cybersecurity top of mind, reducing risks due to human error.

Best practice: Conduct monthly cybersecurity briefings with updated threat information.

Questions to ask:

- Are there ongoing awareness programs to keep staff informed about the latest cybersecurity threats?
- How is information about potential threats communicated to staff?

Awareness checklist:

- Monthly cybersecurity briefings provided.
- Regular threat information updates shared.
- Feedback mechanism for staff to report security concerns.

Training and awareness scorecard:

- Training completeness: __/5
Evaluate the extent and regularity of medical device-specific cybersecurity training provided to staff.
- Training effectiveness measurement: __/5
Assess how effectively training outcomes are measured, including regular evaluations of staff understanding and application.
- Awareness program reach: __/5
Review the frequency and reach of ongoing awareness programs, such as monthly briefings and threat updates.
- Feedback mechanism utilization: __/5
Examine the effectiveness of feedback channels for staff to report security concerns and stay engaged with current threats.



Monitoring & incident detection

1. Monitoring tools:

Why it matters: Monitoring tools detect unusual activity and provide early warnings of potential threats.

Best practice: Integrate monitoring tools with IT security systems for a centralized view.

Questions to ask:

- What tools or systems do you use to monitor the security of medical devices?
- Are these tools integrated with your overall IT security monitoring system?

Monitoring checklist:

- Comprehensive monitoring tools implemented.
- System integration with IT security.
- Alerts configured for unusual activity.

2. Anomaly detection:

Why It matters: Automated detection of unusual behavior helps prevent unauthorized access or data breaches.

Best practice: Configure automated alerts for quick response.

Questions to ask:

- How do you detect unusual or suspicious activity on medical devices?
- Is there an automated alert system for potential security incidents?

Anomaly detection checklist:

- Automated anomaly detection enabled.
- Quick response protocols in place.
- Regular audits to fine-tune detection systems.

3. Incident reporting:

Questions to ask:

- What is the process for reporting cybersecurity incidents involving medical devices?
- Is there a dedicated team or individual responsible for handling these incidents?

Incident reporting checklist:

- A clear process is documented for reporting cybersecurity incidents involving medical devices.
- A dedicated team or individual is assigned to manage incident reporting and response.
- Incident reporting channels are easily accessible to all relevant staff.
- Incident response plan is reviewed & updated annually.
- Incidents are logged and reviewed to identify recurring issues and improve security.
- Post-incident reviews are conducted to strengthen future response efforts.

Monitoring and incident detection scorecard:

- Monitoring tools implementation: __/5
Evaluate the comprehensiveness of monitoring tools and their integration with the overall IT security system.
- Anomaly detection efficiency: __/5
Assess the effectiveness of automated anomaly detection and the promptness of response protocols.
- Incident reporting readiness: __/5
Review the clarity and accessibility of the incident reporting process, along with the presence of a dedicated response team.



Vendor management

1. Vendor evaluation:

Why it matters: Evaluating vendor cybersecurity practices ensures that third-party products and services align with your security standards, reducing risks introduced by external partners.

Questions to ask:

- How do you assess the cybersecurity practices of medical device vendors?
- Are cybersecurity requirements included in vendor contracts?

Vendor management checklist

- Cybersecurity practices of all medical device vendors are thoroughly assessed.
- Cybersecurity requirements are explicitly included in vendor contracts. All staff trained on updated policies.
- Regular reviews of vendor compliance with cybersecurity standards are conducted.

2. Patches and updates:

Why it matters: Properly managing patches and updates protects devices from vulnerabilities that can be exploited by cyber threats, ensuring continuous security.

Questions to ask:

- How do you manage and apply patches and firmware updates provided by vendors?
- Is there a schedule or policy for regular updates?

Patches and updates checklist:

- A clear process is in place for managing and applying patches and firmware updates from vendors.
- A schedule or policy ensures regular updates are applied to maintain security.
- Emergency patch procedures are established for critical vulnerabilities.

3. Third-party assessments:

Why it matters: Conducting third-party assessments identifies vulnerabilities in vendor-supplied devices before deployment, ensuring security standards are met.

Questions to ask:

- Do you conduct third-party security assessments of medical devices before deployment?
- How frequently are these assessments conducted?

Third-party assessment checklist:

- Third-party security assessments are conducted for all medical devices before deployment.
- Frequency of assessments is determined based on risk level and is conducted regularly (e.g., annually or semi-annually).
- Results of assessments are reviewed and factored into cybersecurity planning.

Vendor management scorecard:

- Vendor evaluation thoroughness: __/5
Evaluate how comprehensively vendor cybersecurity practices are assessed and incorporated into contracts.
- Patch and update management: __/5
Assess the effectiveness of patch management procedures, including scheduling and emergency protocols.
- Third-party assessment frequency and review: __/5
Review the regularity and thoroughness of third-party security assessments and the integration of findings into security planning.



Backup and recovery

1. Backup & recovery

Why it matters: Regular backups prevent data loss and ensure quick recovery in case of cyber incidents.

Best practice: Schedule daily backups and test recovery plans quarterly.

Questions to ask:

- Are there backup and recovery plans specifically for medical devices?
- How often are these plans tested?

Backup checklist:

- Daily backups of device data completed.
- Quarterly recovery tests.
- Secure off-site backup storage.

2. Recovery planning:

Why it matters: A clear recovery plan enables quick restoration of medical devices and prevents prolonged downtime.

Best practice: Create a tiered recovery plan prioritizing critical devices.

Questions to ask:

- Is there a detailed recovery plan for medical devices?
- Are critical devices prioritized in the recovery process?

Awareness checklist:

- Detailed recovery plan in place.
- Prioritization of critical devices.
- Regular testing of recovery procedures.

Backup & recovery scorecard:

- Backup protocol completeness: __/5

Evaluate if backup protocols are thorough, reliable, and cover all necessary medical device data.

- Recovery plan effectiveness: __/5

Assess the recovery plan's ability to restore devices quickly and securely, with regular testing to ensure readiness.

Strengthen your cybersecurity posture with Intelas

Thank you for taking the time to explore this Cybersecurity Readiness Toolkit for Medical Devices. By assessing your current practices and identifying areas for improvement, you're taking a proactive step toward safeguarding your medical devices, protecting patient data, and ensuring operational integrity.

At Intelas, we understand the unique challenges hospitals face when managing medical device security. Our comprehensive solutions are designed to support your organization in enhancing patient safety, ensuring compliance, and building a resilient cybersecurity framework.



Let's work together

Partner with Intelas to implement tailored strategies that address your hospital's specific needs. From risk assessments to vendor management and beyond, our Cyber Defense Team provides the expertise and resources to help you achieve a secure and reliable healthcare environment.

Contact us today:

Visit intelashealth.com to learn more about our services and how we help secure medical devices.

Together, we can create a safer, more secure future for your hospital and the patients you serve.