Medical Device Manufacturers and Engineers Security and Privacy Checklist

1. Assign a position or team within your organization with responsibility for ensuring information security and privacy controls are designed and built into all medical devices.
2. Give the assigned position/team the authority to enforce the security and privacy requirements.
3. Document clear and comprehensive information security and privacy requirements and integration procedures.
4. Establish and follow procedures to keep medical device operating systems and software patched.
5. Ensure requirements and procedures mitigate all associated security and privacy risks.
6. Ensure requirements and procedures meet all applicable legal requirements (e.g., HIPAA, FDA, GDPR, etc.)
7. Perform internal vulnerability testing on all devices prior to making available for patient use.
8. Engage an external entity to perform penetration and vulnerability tests on all wireless and data capable medical devices prior to making available for patient use.
9. Establish and consistently follow documented change management processes for medical devices.
10. Encrypt wireless transmissions between medical device and devices communicating with it.
11. Encrypt data within and collected from devices wherever the data is in storage.
12. Do NOT use hard-coded passwords.
13. Do not use weak (e.g., “abcde”, “12345”, “admin”, “password”, etc.) or default passwords.
14. Establish an inactivity automatic logout to prevent unauthorized access.
15. Implement remote-data-wiping capabilities.
16. Incorporate malware protection within data collection and storage devices.
17. Build in data access logging capabilities. *NOTE: There are legal requirements to do this, such as under the Accounting of Disclosures requirements of HIPAA.*
18. Support effective networking security controls.
19. Use Virtual Routing and Forwarding (VRF)/Multi-Protocol Label Switching (MPLS) with firewalls to place medical devices and servers in virtual DeMilitarized Zones (vDMZ) and pass network traffic over Virtual Private Networks (VPN).
20. Isolate wireless networks by using non-WiFi technologies or reserving specific 5.8 GHz channels for IT and medical uses.

21. Design into the device a "fail-safe mode" to maintain the device's critical functionality even when security has been compromised.
22. Establish incident management procedures for threats to the devices, and to the associated data.
23. Do not share data from the medical devices without providing notice to and obtaining consent from the associated patients.
24. Establish security and privacy monitoring capabilities, and associated metrics.
25. Provide regular information security and privacy training, along with ongoing awareness communications, to medical device engineers and sales/ marketing personnel.
26. Provide documentation to medical device clients (doctors, hospitals, etc.) that clearly explain all the information security and privacy controls, how to modify them, and the associated impacts.
27. Ensure all apps and wearable computing devices used with the medical devices have effective information security and privacy controls built in.

Never make assumptions that no one will know how to access data, or will not want data, and decide not to build in security and privacy controls; such assumptions put patient data, privacy, and health at risk!

Just a few examples of medical devices that have data collection and/or storage capabilities, and/or wireless access, include:

- **Life Sustaining Devices**: Defibrillators, Heart-Lung Bypass machines, Intensive Care Unit (ICU) Ventilators, Anesthesia Delivery Systems, Insulin Pumps, Pacemakers etc.
- **Monitoring Devices**: Physiologic Monitors (ICU, Operating Room, Emergency Department, etc.), Vital Signs Monitors, Medical Telemetry, etc.
- **Diagnostic Devices**: Electrocardiographs, MRI Scanners, Computed Tomography Scanners, Pulmonary Function Analyzers, Ultrasound Machines, etc.
- **Treatment Devices**: Infusion Pumps, Surgical Lasers, Linear Accelerators (Radiation Oncology), Dental Instrumentation, Cardiac Catheterization Labs, etc.
- **Therapeutic Devices**: Communication and cognitive devices for physical, sensory, and cognitive disabilities Analytical Devices: Blood-Gas Analyzers, Cell Counters, etc.
- **Tracking Devices**: Fitness trackers, vital signs trackers, some neurological devices, some stent systems, insulin monitoring devices, etc.

Medical Device Security and Privacy Resources:

- FDA Fact Sheet: "The FDA's Role in Medical Device Cybersecurity" https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM544684.pdf
- FDA: "Postmarket Management of Cybersecurity in Medical Devices" https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf
- Technical Considerations for Additive Manufactured Devices - Draft Guidance for Industry and Food and Drug Administration Staff https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM499809.pdf
- The 3Rs of 3D Printing https://www.fda.gov/ForConsumers/ConsumerUpdates/ucm533992.htm
- FDA Medical Devices Page https://www.fda.gov/medical-devices
- FDA Medical Devices Recalls https://www.fda.gov/medical-devices/medical-device-safety/medical-device-recalls
- NIST Medical Device "Body Area Networks & Pervasive Health Monitoring" projects: https://www.nist.gov/healthcare/emerging-technologies-healthcare/body-area-networks-pervasive-health-monitoring
- NIST SP 1800-8: Securing Wireless Infusion Pumps In Healthcare Delivery Organizations https://www.nist.gov/programs-projects/emerging-technologies-healthcare/body-area-networks-pervasive-health-monitoring
- NISTIR 8259 (Draft) January 2020: Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline (2nd Draft) https://csrc.nist.gov/publications/detail/nistir/8259/draft
- Cybersecurity for Medical Devices and Hospital Networks: https://www.fda.gov/medical-devices/digital-health/cybersecurity

This complimentary assistance is provided by:

- The Privacy Professor® Consultancy https://www.privacyguidance.com
- Privacy Security Brainiacs Security, Privacy, IT & Compliance Tools and Services https://www.privacysecuritybrainiacs.com

For more information:

- Rebecca Herold, CEO, The Privacy Professor: rebeccaherold@rebeccaherold.com
- Noah Herold, Web and Applications Development Director NoahHerold@privacysecuritybrainiacs.com