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 risks.
6. Ensure requirements and procedures meet all applicable legal requirements (e.g., HIPAA, FDA, 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.
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. Establish an inactivity automatic logout to prevent unauthorized access.
15. Incorporate malware protection within data collection and storage devices.
16. Build in data access logging capabilities. NOTE: There are legal requirements to do this, such as under the Accounting of Disclosures requirements of HIPAA.
17. Support effective networking security controls. E.g.,
   a. 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)
   b. Isolate wireless networks by using non-WiFi technologies or reserving specific 5.8 GHz channels for IT and medical uses
18. Design into the device a "fail-safe mode" to maintain the device’s critical functionality even when security has been compromised.
19. Establish incident management procedures for threats to the devices, and to the associated data.
20. Do not share data from the medical devices with providing notice to and obtaining consent from the associated patients.
22. Provide regular information security and privacy training, along with ongoing security and privacy awareness communications.
23. Provide documentation to medical device clients (doctors, hospitals, etc.) that clearly explains all the information security and privacy controls, how to modify them, and the associated impacts.
24. 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.