# Cyber Threats to Medical Technology *and* Communication Technology Protocols

Healthcare facilities utilize a variety of medical devices ranging from immobile imaging machines and mobile workstations to wearable or implanted mobile devices capable of sending and receiving data over various communications protocols. The increasing cyber threats targeting the Healthcare and Public Health sector place these devices at a greater risk of disruption, degradation, and destruction. The Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) developed this infographic to show examples of cyber threats related to the expansion of the interoperable IT/OT environment in healthcare and the potential consequences.

## Device Data Flow Examples

### Pacemaker

- Implanted device connects to at-home transmitter and/or clinician programmer via Bluetooth or radio frequency
- Transmitter or programmer sends data via Wi-Fi or cellular connection to EHR or clinician management portal
- Implanted device is accessible via clinician programmer or patient device (e.g., smart phone or at-home transmitter)

### Smart Infusion Pump

- Connects to hospital internal network via Wi-Fi or ethernet
- Transmits status, alerts, and alarms to central monitoring/control station, and transfers data to EHR

### MRI

- The MRI machine may be connected to the hospital's internal network
- Scans may be encoded and sent to PACS software via DICOM
- PACS images may be stored locally and made available on web based EHR
- Images may be available to clinicians on network devices including computer workstations, tablets, and smart phones

**Legacy and end-of-service OT may** expose the network to exploitable entry points and potentially leaves vulnerabilities unpatched.

**Artificial Intelligence (AI) and Machine Learning (ML)-enabled medical devices may be** vulnerable to cyber incidents targeting data such as data poisoning, theft of personal and proprietary data, and modifying AI or ML parameters to inject backdoors.

**Bluetooth-enabled devices** may lack data encryption protocols which could allow eavesdropping. Bluetooth implementations may not limit command requests which could cause battery drainage or denial of service.

**OT devices** may not be segmented within the hospital network which could allow unauthorized lateral movement across the network and pivoting to alternative devices.

**IoT devices** may not support data encryption, may allow cleartext data transmission, or may store passwords in plaintext which could allow unauthorized users to connect to the device to access data, alter system configurations, alter communications protocols, or cause device malfunction.

**Third-party vendors** with remote device access could be access points for unauthorized actors seeking access to the hospital network.

**Medical software, such as DICOM and PACS, may** lack proper input validation which could allow unauthorized access or may transmit data in cleartext and use poor cryptographic algorithms which could lead to path traversal and allow unauthorized actors to view or modify data.

**Radio frequency (RF) interference** can degrade device communications channels, cause data loss, and misinterpretation.

**5G wireless connectivity** will introduce vulnerabilities to a healthcare network through hardware and software supply chains and the expansion of the potential attack surface in a healthcare facility.

**Risk Mitigation Resources:**

Mitigation measures: Conduct risk assessments (https://aspr.hhs.gov/cip/hph-cybersecurity-framework-implementation-guide/Pages/default.aspx), practice effective IT procurement (https://www.fda.gov/medical-devices/guidance-documents-medical-devices-and-radiation-emitting-products/recent-final-medical-device-guidance-documents), and follow HIPAA security and management standards (https://csrc.nist.gov/pubs/sp/800/66/r2/ipd). General cybersecurity guidance is provided through HHS's 405(d) (https://405d.hhs.gov/information), the NIST Cybersecurity Framework (https://www.nist.gov/cyberframework), and CISA's HPH Cybersecurity Toolkit (https://www.cisa.gov/topics/cybersecurity-best-practices/healthcare), CISA's Mitigation Guide: Healthcare and Public Health Sector (https://www.cisa.gov/resources-tools/resources/mitigation-guide-healthcare-and-public-health-hph-sector), and CISA's HPH Sector Risk and Vulnerability Assessment (https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-349a).