AdvaMed
The Medtech Association

Remote Device Operations:
Common Challenges and Mitigation Strategies

Effective remote management of medical devices requires awareness and proactive handling of technical and operational issues that arise frequently. Healthcare providers must understand these common challenges and collaborate with device manufacturers and IT teams to mitigate disruption and maintain device efficiency and safety.

Interoperability and Standards

Interoperability of medical devices and other IT equipment in an IT health infrastructure is a shared responsibility of multiple stakeholders. IEC 80001-1 provides the framework to establish safety, effectiveness, and security in the implementation and use of connected medical devices and software. ISO TR 80001-2-6 provides guidance to establish responsibility agreements. When implementing remote solutions, manufacturers are advised to consider the ANSI/AAMI/UL 2800 series of standards and ensure agreements for integration and maintenance.

Definitions

Peripheral Devices:
External devices like keyboards, mice, scanners, and monitors that connect to a computer.

Kiosk Mode:
A computer setting that limits user access to specific applications or functions.

Firmware:
Software programmed into hardware devices that controls basic functions.

Absolute Mouse Mode:
A setting where mouse movement corresponds directly to screen position, used in certain remote setups.

HID Interfaces:
Human Interface Devices like keyboards, mice, and touchscreens.

KVM Devices:
Hardware that lets users control multiple computers with one keyboard, video monitor, and mouse.

VPN:
A Virtual Private Network that securely connects a user to a network over the internet.

Peripheral Device Challenges

Peripheral device compatibility remains a prevalent issue, including unrecognized input devices like mice due to outdated software or kiosk-mode restrictions. Latency can introduce usability challenges, such as display freezing, pixelation, or misalignment of input devices. While temporary fixes, such as restarting viewers or scanners and maintaining stable power supplies (UPS), provide immediate relief, permanent solutions require collaboration with hardware and software providers.

Software Compatibility Issues

Remote operations frequently face compatibility issues such as outdated drivers, mismatched operating systems, and firmware discrepancies. Absolute mouse mode incompatibility in kiosk-mode or older scanner systems often impacts usability. Providers must ensure regular updates, especially of graphics drivers, while working around security restrictions.

Network-Related Issues

Bandwidth limitations, unstable video feeds, and audio degradation are frequent challenges. Providers must define network requirements, close unnecessary apps, and coordinate with IT to establish robust network protocols and monitoring.

Third-Party Hardware Integration

Improper screen scaling and audio device mismatches are common. Close coordination with hardware suppliers is critical to ensure remote workstations are optimized and hardware compatibility is proactively addressed.

Third-Party Remote Interaction Tools

KVMs and web viewers often face compatibility problems on older systems or secure browsers. Providers should ensure tool developers align with current security and compatibility standards.

Security Patches and Updates

Security updates may reset settings or misalign peripherals. Providers must anticipate and plan for post-update configurations in coordination with IT and vendors to reduce downtime.

Cloud Infrastructure Challenges

Cloud deployments can introduce latency and integration issues due to shared resources and data center distance. Jurisdictional data residency laws and cost unpredictability further complicate adoption. Coordination with vendors is essential.

Post-Service Update Issues

Medical imaging equipment manufacturers' servicing and maintenance procedures may require remote control functionality to be disconnected. Imaging equipment service personnel may not be trained or qualified to reestablish remote capabilities. Providers are encouraged to define clear protocols with technicians and manufacturers of the remote operations hardware and software for resolution.

Service updates to the equipment involved in remote operations may also impact compatibility between those devices. This can affect remote operation functionality.

Other Common Challenges

Security barriers, bandwidth constraints, and unoptimized workstations continue to impact performance. Providers should standardize protocols for managing these issues.

Additional Considerations

Vendors may resist changes citing regulatory implications. Legal and liability issues, vendor-imposed restrictions on HID interfaces, and customer infrastructure limitations (e.g., VPNs, static IPs) also pose hurdles. Deployments across state or country lines remain limited by current regulations.

Remote operation of medical devices introduces multiple technical and operational challenges. Addressing these proactively—through collaboration with IT, vendors, and regulatory stakeholders—is essential for long-term reliability and efficiency.