Medical Imaging Device Cybersecurity: Critical Outage Situations and Response

Technical Performance & Safety Whitepaper

Published by: **AdvaMed - Advanced Medical Technology Association** 1301 Pennsylvania Avenue NW #400,
Washington, DC 20004
www.advamed.org

AdvaMed
The Medtech Association

Medical Imaging Device Cybersecurity: Critical Outage Situations and Response

Technical Performance & Safety Whitepaper

1. Defining Minimum Viable Product: Fulfilling the Intended Use

In an outage scenario, the minimum viable product (MVP) for a medical imaging device is its ability to maintain its essential performance despite disruptions in power, network connectivity, or external system dependencies. The core function of these devices is to acquire, process, and display images critical for clinical decision-making. Any failure that prevents these fundamental operations from continuing, even in a limited capacity, compromises patient care and disrupts clinical workflows.

Beyond image acquisition and storage, ensuring continued usability is also critical. User interfaces must remain functional, allowing radiologists and technicians to interact with the system without requiring cloud-based access or remote authentication services. Essential safety features, such as cooling systems in Magnetic Resonance Imaging (MRI) machines or radiation dose monitoring in Computed Tomography (CT) scanners, must remain active to prevent harm to patients and operators. In short, the MVP in a critical outage is not simply about keeping the system powered on but ensuring that it can still perform the core medical function for which it was designed. The design of medical imaging devices must account for these scenarios, integrating fallback mechanisms that allow continued operation in a reduced but clinically effective state.

2. Understanding ‘Limited’

Understanding what "limited" means in different outage scenarios is crucial for designing resilient systems. While temporary workarounds can allow continued operation, they should be anticipated and planned for to ensure that any reduction in functionality does not compromise patient care or clinical efficiency.

3. General Workflow Impacts

One of the most immediate impacts of a network outage is the delay in transmitting imaging results to remote physicians and specialists. In a connected system, radiologists can rapidly interpret scans and share findings electronically with referring providers. However, when network access is lost, these results may need to be manually transferred using external storage devices or printed copies, increasing the time between image acquisition and clinical decision-making. This delay can be particularly critical in emergency settings where rapid diagnosis is essential for patient outcomes.

Within imaging departments, the lack of network connectivity often necessitates a shift to manual documentation and scheduling processes. Without automated integration with Hospital Information Systems (HIS), technologists and administrative staff may need to rely on paper-based request forms, handwritten patient records, or local spreadsheets to track imaging orders and results. This not only increases the workload but also introduces the potential for communication gaps or overlooked information, which may affect patient safety and operational efficiency.

To mitigate these disruptions, healthcare providers must establish contingency plans that allow for continued imaging access and result retrieval during outages. Offline access to imaging data, manual scheduling workflows, and predefined protocols for transferring critical patient information can help ensure continuity of care. While temporary solutions can minimize workflow disruptions, designing imaging devices with built-in resilience and redundancy is essential to maintaining efficiency and patient safety in the face of network failures.

4. Transition from Network-Connected to Local-Only Mode

When an imaging device transitions from network-connected operation to local-only mode, several critical aspects of its functionality and serviceability are affected. This shift alters how images are stored and shared, impacts support and maintenance capabilities, and could introduce challenges related to software security and data management. While the device may remain operational for imaging, its ability to integrate with the broader healthcare system is significantly reduced, requiring manual interventions and contingency measures.

One of the most immediate changes is the loss of automated connectivity to hospital networks and external systems such as Picture Archiving and Communication Systems (PACS) and HIS. Without network access, imaging devices can no longer transfer images automatically, forcing radiology staff to handle data manually using external storage devices or other temporary solutions. This not only increases workflow complexity but also introduces risks related to data integrity and timely access to imaging results.

Data management also becomes another concern. With images and patient information stored locally, hospitals and imaging centers must ensure that there is adequate on-device storage and a robust backup strategy to prevent data loss. If storage capacity is exceeded or backup procedures are inadequate, valuable diagnostic data could be at risk. Proper contingency planning is essential to maintaining safe and effective operations when an imaging device transitions to local-only mode.

5. Service Level Agreement (SLA) Impacts

Service level agreements (SLAs) are formal contracts between medical device manufacturers and healthcare providers that define expectations around device performance, service availability, and support response times. These agreements are often customized and may be established at the time of procurement or applied to an existing device fleet.

SLAs commonly address responsibilities related to software maintenance, cybersecurity protections, system uptime, and remote diagnostics. In many cases, they also specify how quickly a manufacturer must respond to issues and what support services are guaranteed during standard and after-hours periods.

A typical SLA may include manufacturer commitments for:

- Coverage periods (days and times of standard coverage)
- After-hours coverage periods
- Uptime guarantees
- Parts coverage
- Remote service
- Planned maintenance
- Assurance services
- Updates
- Phone support
- Response times

Additional terms may be negotiated based on provider needs and the device type. However, during a cybersecurity event or network outage, these agreed-upon terms may not be fully enforceable. Depending on the nature of the disruption, some SLA obligations may be suspended, and timelines for service delivery could be extended.

For instance, if a provider takes a device offline for cybersecurity containment, the manufacturer may be unable to deliver automatic updates, remote service, or timely diagnostics. If the provider's entire network is down, scheduling service calls or delivering parts may also be delayed. Likewise, any guaranteed uptime targets would be difficult to maintain. On the other hand, if the disconnection is on the manufacturer’s side, the provider may experience similar impacts—delays in phone support, extended response times, and missed assurance activities.

Regardless of who initiates the disconnection, both parties must recognize how these events affect contractual obligations. Clear communication and a mutual understanding of SLA limitations during outages are essential for realistic planning and continued patient safety. When operating in local-only mode, providers and manufacturers should revisit service expectations and adjust as necessary to ensure appropriate device support and clinical continuity.

Ransomware Infection of an Imaging Device

Medical imaging devices like MRI and CT scanners are vital components of modern healthcare infrastructure. These systems are used daily for diagnosis, treatment planning, and ongoing clinical care. Because of their high cost, healthcare providers often continue to use these devices well beyond their official end-of-life (EOL) or end-of-support (EOS) periods. This practice introduces significant cybersecurity challenges. Once a device no longer receives regular security updates, it becomes increasingly vulnerable to threats such as ransomware.

Ransomware attacks on imaging devices can lead to serious operational disruptions. They can delay critical diagnoses and interrupt patient care if key imaging services become unavailable. Imaging devices are deeply integrated with hospital networks and often depend on real-time communication with systems like electronic health records (EHRs) and PACS. This interconnectedness increases the risk that a single compromised device can serve as a launch point for broader network infection. Compounding the issue, imaging systems often run proprietary software on unique hardware configurations, making recovery more complex than for standard IT devices.

Challenges

Imaging devices that have exceeded their support lifecycle face a higher risk of unresolved infections. These systems often operate on outdated platforms, such as Windows XP or Windows 7, which no longer receive vendor support or security patches. Endpoint protection tools may not be compatible with these operating systems, limiting the ability to defend against or detect ransomware. Additionally, regulatory and safety requirements often prevent rapid patching, meaning these systems may remain exposed longer than typical IT endpoints.

Even after remediation, these systems may be at risk of re-infection if the network contains other compromised assets. Many ransomware variants use lateral movement tactics to reinfect previously cleaned devices. Imaging systems that interact with shared systems like PACS, radiology information systems (RIS), or hospital IT networks can act as points of reinfection if not properly secured. Without advanced protections—such as application whitelisting or behavior-based anomaly detection—the risk of recurring compromise remains high.

Remediating ransomware infections in imaging systems is also more complex than with general-purpose computers. Imaging devices often require manufacturer support for system restoration, calibration, and compliance validation. IT staff may be unable to intervene directly due to regulatory requirements or warranty restrictions. This dependency on vendor support can delay system recovery, especially when multiple devices are affected or during high-demand periods. Restoration processes must not only eliminate the threat but also ensure the system continues to meet clinical and regulatory standards, further increasing complexity and downtime.

Response Plan

A clear, well-defined response plan is crucial to mitigate the impact of a ransomware attack on medical imaging devices. Recovery efforts must balance cybersecurity containment with the need to restore clinical operations safely and quickly.

1. Isolate the Infected Device

The first step is containment. The infected device should be disconnected from the hospital's network—whether wired or wireless—to stop the spread of ransomware. Logical isolation may involve disabling network interfaces while allowing for forensic analysis. It is also essential to prevent the device from accessing shared systems like PACS, RIS, and EHR platforms. Because these devices operate in tightly connected environments, isolation efforts should be coordinated among cybersecurity, IT, and clinical engineering teams to ensure patient care is not unnecessarily disrupted.

2. Restore from Trusted Backups

Once isolated, the next priority is to restore the device from a clean, trusted backup. Backup integrity must be verified before use, with checks to ensure the restored system isn't reintroducing vulnerabilities. In some cases, older backups may lack necessary security patches, so patching and hardening steps must follow restoration. Before going back online, the system should be scanned using malware detection tools to confirm it is safe. A phased restoration approach—starting with essential services—can help validate the process without risking full reinfection.

3. Coordinate with Device Manufacturers

Due to the complexity and regulatory sensitivity of imaging devices, manufacturer involvement is often required for restoration. Vendors can provide validated recovery processes, reinstall proprietary software or firmware, and help ensure regulatory compliance is maintained. Coordination with the manufacturer also ensures that any outstanding vulnerabilities are patched during recovery. Skipping this step may result in incomplete remediation and continued system exposure.

4. Implement Network Segmentation

To prevent future incidents, network segmentation strategies should be applied to imaging systems. These devices should be placed on separate VLANs, with communication restricted to essential systems only. Firewalls, access control lists, and zero-trust principles can reduce exposure to broader network threats. External communication should be limited, and unused ports and protocols should be disabled by default. These steps help contain future infections and prevent ransomware from spreading across the hospital network.

Device Disconnected from an Internal Network Infected by Ransomware

When a medical imaging device is deliberately or automatically disconnected from an internal hospital network due to a ransomware incident, the consequences are immediate and disruptive. These devices depend on seamless integration with hospital information systems (HIS), electronic health records (EHRs), and Picture Archiving and Communication Systems (PACS) to function efficiently within clinical workflows. Once disconnected, the imaging device becomes isolated—not only from cybersecurity threats but also from the digital ecosystem that supports timely clinical decision-making.

Challenges

This disconnection, though necessary to protect the device from infection, has a significant impact on patient care. One of the primary consequences is clinical delay. Physicians and other healthcare providers may not receive imaging results in a timely manner, as automated image transmission to PACS or the EHR is no longer possible. In situations where time-sensitive diagnoses are critical—such as stroke assessments or trauma evaluations—these delays can directly affect patient outcomes.

Radiology departments may find themselves burdened with additional coordination tasks: tracking orders manually, labeling physical storage devices, and ensuring that results are hand-delivered to the appropriate care team. In busy clinical environments, this added complexity can lead to backlog, misrouted images, and patient frustration.

Response Plan

Pre-established continuity plans are critical in these situations. Radiology departments should maintain protocols for managing imaging requests, assigning priorities, documenting transfers, and verifying that results reach the intended providers. These protocols should be simple, accessible, and familiar to staff so they can be implemented quickly under pressure. They should also account for data protection practices to prevent mishandling of patient information during physical transfers.

In addition, immediate notification of IT and cybersecurity teams is necessary once a device is taken offline. Prompt alerting ensures that network recovery efforts can begin, including threat containment, system integrity assessments, and plans to reconnect clean systems. IT teams must be included early to assess the scope of the infection, validate that imaging devices remain uninfected, and coordinate a secure path back to normal operations.

Device Disconnected from Internet Access

In many cases, medical imaging devices such as CT, MRI, or ultrasound systems are designed to operate independently of internet access for their core clinical functions. These devices typically do not require an internet connection to perform image acquisition, processing, and display—all essential elements for diagnosis and treatment planning. However, the loss of internet connectivity can still have a notable impact on overall functionality, particularly for services that depend on cloud-based systems or remote connectivity.

Challenges

A key area affected by internet disconnection is remote technical support. Many imaging devices today are supported by manufacturers or service vendors who offer remote diagnostics, performance monitoring, and troubleshooting services. When internet access is lost, these capabilities are disrupted. Without remote access, service teams cannot identify or resolve issues quickly, often requiring on-site support instead. This shift may extend downtime or delay service response, especially in facilities that rely heavily on remote support for day-to-day operations.

Another consequence is the interruption of cloud-based software updates, including critical security patches. These updates are often scheduled and deployed automatically when internet access is available. Without connectivity, devices may continue operating on outdated software, potentially exposing them to security vulnerabilities or missing performance enhancements. This delay becomes more serious during prolonged outages, when patching gaps may increase over time. In regulated environments, the inability to receive timely updates may also present compliance concerns, particularly with respect to cybersecurity best practices and maintenance obligations under applicable laws or standards.

Response Plan

When internet access is lost, the immediate goal should be to ensure that the imaging device remains fully operational for its primary clinical purpose. Facilities should verify that image acquisition, review, and storage can continue using local networks and storage systems. Most imaging devices are designed with this independence in mind, and on-premise functionality should be prioritized to avoid disruptions to patient care. If cloud-based reporting or AI features are affected, alternate workflows should be identified so that radiology services can continue uninterrupted.

Finally, any effort to restore internet connectivity must be done securely. Healthcare organizations should work closely with IT and cybersecurity teams to reestablish internet access in a controlled and secure manner. This includes scanning systems for potential threats, validating device configurations, and ensuring that security controls such as firewalls, authentication protocols, and monitoring tools are properly configured. Reconnecting devices without proper safeguards may expose systems to new vulnerabilities, especially in the aftermath of a broader cybersecurity event.

Corrupted Updates

Medical imaging devices rely on tightly controlled software and firmware to function accurately and reliably. When a software update is corrupted—whether due to incomplete installation, network disruption, or malicious tampering—the result can be highly disruptive. Corrupted updates may impair core functions such as image acquisition, processing, or display, and in some cases, may cause total device failure. Even partial corruption can lead to unstable system behavior, including crashes, error messages, or degraded image quality, all of which can compromise clinical confidence and delay patient care.

Corruption during updates is particularly concerning in environments where imaging devices are integrated into broader hospital systems and must meet high standards of performance and reliability. Because these devices support critical diagnostic functions, any instability can create ripple effects throughout the healthcare delivery process. For example, if a CT scanner begins producing inconsistent images or cannot complete scans due to a software malfunction, clinicians may be forced to reschedule exams, refer patients to other facilities, or use alternate imaging methods that are less optimal for the clinical need.

Challenges

The challenges posed by corrupted updates are multifaceted. The most immediate concern is device downtime. Troubleshooting the cause of the issue—whether it's a software bug, compatibility error, or the result of a tampered update—can take time. Imaging devices often require specialized diagnostics and service procedures that must be performed either by the manufacturer or an authorized technician, and this dependency can lead to extended outages.

Another significant challenge is regulatory compliance. Imaging devices must operate within strict performance and safety standards, and a non-functional or unstable device may fall outside of these boundaries. This could result in the device being temporarily removed from clinical use, with associated reporting and documentation obligations. In regulated healthcare environments, failure to properly address software issues could lead to findings during audits or even compromise accreditation.

Response Plan

The first step in addressing a corrupted update is to roll back the system to a previous, known-good configuration. Many imaging devices include features that allow for restoration to a baseline software version or system image, but this process often requires manufacturer involvement. It is essential to verify that the restored version meets current clinical and security requirements, as rolling back too far may reintroduce known vulnerabilities or performance limitations.

Once stability is restored, verifying the integrity of the update process is crucial. All future updates should be retrieved from trusted, authenticated sources. This may involve checking digital signatures, using secure update delivery platforms, and ensuring the update file has not been altered in transit. Facilities should avoid using any update files that were downloaded during periods of known network instability or potential compromise, as these may carry hidden risks.

Ongoing collaboration with the device manufacturer is vital. Manufacturers can provide diagnostic tools, validated recovery procedures, and insights into whether the issue is isolated or part of a broader pattern. In some cases, the manufacturer may need to reimage the system, recalibrate critical components, or conduct post-restoration testing to ensure compliance with regulatory standards.

Hardware Outage Situations

Medical imaging devices are highly complex systems that rely heavily on integrated storage components—such as hard drives, solid-state drives, or non-volatile RAM—to store operating systems, software applications, patient data, exam orders, and imaging results. These storage components are essential to the core functionality of the device. If the local storage system fails, the impact is immediate and severe. In many cases, the entire device becomes inoperable, and previously stored data may be lost or corrupted, directly affecting diagnostic workflows and potentially compromising patient care.

Challenges

One of the most critical challenges associated with hard drive failure is the risk of losing patient data. If the device has not been regularly backing up data, important scans, reports, and configurations may become unrecoverable. This compromises continuity of care and may require repeat imaging, which adds time, cost, and potential radiation exposure for patients.

Another major challenge is total device failure. When the hard drive hosting the operating system or clinical software fails, the device may become unusable until the hardware is replaced and the system is fully restored. This is especially impactful in high-throughput environments such as emergency rooms or oncology centers, where downtime can quickly cascade into broader delays in the care continuum.

Response Plan

To prevent and manage hard drive failures effectively, manufacturers and healthcare providers must adopt a combination of preventive, detective, and responsive strategies. Preventive measures start with ensuring that imaging systems are installed, handled, and operated under stable, specified environmental conditions. This includes maintaining appropriate temperature, humidity, and protection from vibration or impact. Manufacturers should clearly document these requirements so that healthcare facilities can take proactive steps to protect their equipment.

Detection is equally important. Manufacturers should design imaging systems to perform routine internal checks for early warning signs of storage degradation. For example, automated boot-time diagnostics can assess hard drive health before enabling clinical functions. If a failure or restriction is detected, users must be clearly informed —via on-screen messages, device alerts, or log records—about the constraints to the device's intended use or any limitations in supporting infrastructure functions. This helps prevent the use of impaired devices during critical procedures.

In terms of response, redundancy should be built into the system. Imaging devices can be designed with features such as RAID configurations or caching systems that allow for continued operation in the event of partial storage failure. In addition, devices should be configured to automatically back up critical data to secure storage locations —whether that's a second local drive, a hospital data server, or the cloud.

When a failure occurs, rapid recovery protocols must be in place. These include predefined procedures for entering a safe or degraded mode of operation, replacing failed components, and restoring systems from trusted backups. Manufacturers should support this process by providing tools and documentation for restoring both software and configuration data. Post-mortem analysis capabilities should also be available to attempt data recovery from the damaged component and identify the root cause of the failure.