

February 27, 2026

Dear Valued Customer,

This letter is to inform you that effective January 1, 2026; STERIS will no longer fully support the following products as we consider them **Service Obsolete**:

- Clarity Media Repository
- Clarity Modality Tracker
- Clarity Physician View
- Clarity Nurse CoreView
- Standalone CoreView
- Clarity Vitals View
- 24/7 recording of IP Cameras
- Custom CoreView deployments
- Clarity Remote Proctoring

STERIS discontinued sales of these products in March of 2023, with the introduction of HexaVue™ Connect Software Suite. Certain critical software, firmware updates, and patches for these products are no longer available; as a result, STERIS Technical Support's ability to troubleshoot, diagnose, and resolve issues may be limited.

The policy with respect to the support of these products is as follows:

- As of **January 1, 2026**, all Customers under a parts and labor service contract with STERIS will receive parts and labor support on the obsolete products to the extent parts are available for the time remaining on the Customer's current service contract, with no guarantee of parts availability. A labor only service contract is the only option available for this product at contract renewal.
- As of **January 1, 2026**, all Customers under a labor only service contract with STERIS will continue to receive full labor support on the obsolete products through the end of the term of the Customer's current service contract. A labor only service contract will remain available for contract renewal.
- As of **January 1, 2026**, any Customer that is not under a service contract with STERIS yet requires service on a time and material basis will receive parts and labor services based on the resources available at prevailing market prices, with no guarantee of parts availability.
- As of **January 1, 2026**, several services will no longer be provided for these products:
 - New software releases will not be developed. As a result, new security patches and updates, operating system updates, bug fixes, and functional enhancements will not be delivered.
 - Firmware updates will not be developed.
 - Vulnerability assessments and compatibility testing with third-party software components and operating systems will not be performed.
 - Configuration changes driven by updates to the hospital's network or EMR system will not be supported.
 - Technical assistance for cybersecurity-related issues will not be provided.

Cybersecurity Risk Statement for Obsolete Product

The products listed above use obsolete or unsupported operating systems. Obsolete and unsupported operating systems may have inherent vulnerabilities. Without ongoing security updates to its operating system, these products become increasingly vulnerable to exploitation of potential cybersecurity vulnerabilities. Cybersecurity exploitation can result in a risk of compromise to confidentiality, integrity, and availability of data and/or impact clinical workflows. Continuing to use the products listed above constitutes acceptance of any and all residual cybersecurity risks associated with an obsolete product. You should evaluate whether ongoing use aligns with your risk tolerance and clinical operational requirements.

Recommended Actions for Our Customers

Replacement of Obsolete Product

To help maintain security and performance, we highly encourage you to consider upgrading to STERIS HexaVue Connect Software Suite. Your STERIS Sales Representative can help develop a transition plan to replace your existing equipment.

Customer Technical and Physical Security Controls

We encourage you to review your internal policies and risk management strategies to ensure continued patient safety and regulatory compliance and to maintain a secure and safe environment. STERIS recommends that medical facilities implement an information security program based on NIST, HITRUST, or another industry-recognized security framework to ensure robust administrative controls. To reduce potential cybersecurity risks, STERIS recommends implementing the following compensating controls:

- **Boundary Protection** – Implement robust boundary protection measures, including network segmentation and firewall configurations, to safeguard the integrity of data processed by Clarity and CoreView. Implement strict outbound firewall rules to control which systems and services are allowed to initiate SSH connections. Limiting outgoing SSH traffic to specific trusted IP addresses or networks can help prevent unauthorized connections. Continuously monitor network segments to which the products are connected for anomalous activity and review product audit logs.
- **Network Traffic Limitation** – Limit network traffic through meticulous network and firewall configuration to ensure secure communication channels and prevent unauthorized access to sensitive information. Employ the principle of least functionality to network traffic to and from Clarity and/or CoreView by Customer network and firewall configuration.
- **Domain Services Management** – Proper management of domain services, including DNS and Active Directory (AD) integration, streamlines user authentication processes and enhances system security within the hospital environment. Account management policies should employ the principle of least privilege using role-based security for any additional accounts added.
- **Intrusion Detection and Prevention Systems (IDPS)** – Deploy IDPS solutions to monitor network traffic and detect any suspicious activity or attempts to exploit the vulnerability in real-time.

STERIS strives to provide the highest level of Customer support in the industry. As part of our ongoing effort to better serve our Customers, we want to inform you of our policy regarding part/product obsolescence and our product management philosophy.

There are many factors that contribute to our overall product management philosophy. Rapid advancements in technology, the ever-changing standards of care, and the multitude of mandates regarding regulatory compliance are just a few of the market drivers that factor into our overall decision-making process. We continually strive to incorporate advancements in technology and shape best practice standards to not only better serve our Customers but ultimately provide solutions to the marketplace that put patient safety at the forefront.

We recognize the impact that an obsolescence notification has on your operation. To ensure your operating needs are met, please contact a STERIS Sales Representative to arrange a meeting to develop a cost-effective program to replace your existing equipment.

Sincerely,

Tumi Oredein
Equipment Service Sr. Product Manager