



May 27, 2026

Dear Valued Customer,

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

Operating Room Video Integration System (PMCL – 764327291/01)
See Model Numbers below

STERIS discontinued sales of Harmony iQ Integration Systems (“Integration System”) and has since introduced the **HexaVue™ IP & Focus Integration Systems**. Certain critical replacement parts, software, firmware updates and patches for the IDSS Integration System are no longer available. In addition, prices and lead time for the remaining parts and service contract may increase significantly due to low volume production and technological obsolescence.

The policy with respect to the support of this product is as follows:

- As of **June 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 **June 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 **June 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 **June 1, 2026**, several services will no longer be provided for these Integration Systems:
 - 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.
 - New firmware updates will not be developed.
 - Vulnerability assessments and compatibility testing with third-party software components and operating systems will not be performed.
 - Technical assistance for cybersecurity-related issues will not be provided.

Cybersecurity Risk Statement for Obsolete Product

These Integration Systems use obsolete or unsupported operating systems. Obsolete and unsupported operating systems have inherent vulnerabilities. Without ongoing security updates to its operating system, the Integration System becomes increasingly vulnerable to exploitation of cybersecurity vulnerabilities. Cybersecurity exploitation of an OR integration system can result in a risk of compromise to confidentiality, integrity, and availability of data and/or impact clinical workflows. Continuing to use the Integration System 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 a supported STERIS OR integration system. 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 your Integration System. If applicable, 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 the Integration System 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.
- **Access Controls** – Ensure physical security and prevention of unauthorized access to the Integration System, safeguarding patient data stored within the platform. Hospital policy needs to ensure proper authentication and physical controls for remote PCs accessible through the Integration System, as applicable.
- **Retention Policies** – Retention policies for the Integration System recorder's procedure data, media, and logs are essential for system availability and proper operation. Custom data retention policies, if applicable, were implemented per Customer retention requirements provided to STERIS in writing at initial system installation.

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

Systems Covered by this Communication

RLJLM2251R4FC
RLJLM2252R4FC
RLJLM2253R4FC
RLJLM2288R412
RLJLM2288R414
RLJLM2288R415
RLJLM2288R416
RLJLM2288R417
RLJLM2288R418
RLJLM2288R423
RLJLM2288R437
RLJLM2303R301
RLJLM2303R302
RLJLM2303R303
RLJLM2303R304
RLJLM2303R305
RLJLM2303R306
RLJLM2303R307
RLJLM2303R308
RLJLM2328R1
RLJLM2334R301
RLJLM2334R302
RLJLM2334R303
RLJLM2334R304
RLJLM2334R305
RLJLM2334R306
RLJLM2334R307
RLJLM2341R12
RLJLM2342R12
RLJLM2343R22
RLJLM2344R22

RLJLM2349R109
RLJLM2350R110FC
RLJLM2351R111
RLJLM2352R120
RLJLM2352R121
RLJLM2352R122
RLJLM2353R134
RLJLM2421R4
RLJLM2422R4
RLJLM2423R4
RLJLM2424R4
RLJLM2425R32
RLJLM2426R4
RLJLM2427R4
RLJLM2428R32
RLJLM2429R32
RLJLM2439R501
RLJLM2439R502
RLJLM2439R503
RLJLM2439R506
RLJLM2439R507FC
RLJLM2439R509
RLJLM2439R510
RLNMH4FEIN1
RLNMH6OCP1
RLNMH6OCP1FC
RLNMH78OCP1
RLNMH78OCP1FC
RLQ2400BUV3
RLQ2400BUV4
RLQ2800BUD3

RLQ2800BUD4
RLQ2800BUD4FC
RLQ2800BUD4I
RLQ2800BUV3
RLQ2800BUV4
RLQ2800BUV4FC
RLQ2800BUV4UPG
RLQ36008MPH
RLQ3600BUD1FC
RLQ3600BUD3
RLQ3600BUD3FC
RLQ3600BUD4
RLQ3600BUD4FC
RLQ3600BUD4I
RLQ3600BUD5
RLQ3600BUD5FC
RLQ3600BUV1FC
RLQ3600BUV3
RLQ3600BUV4
RLQ3600BUV5
RLQ3600UPGRC2
RLSPERSKY832908
VTLP000335FC
VTLP002204
VTLP002212
VTLP002213
VTP002203
VTP002212
VTP002213