Date: **July 31, 2025**
Product: EVIS EUS ENDOSCOPIC ULTRASOUND CENTER
Model : EU-ME2, EU-ME2 PREMIER, EU-ME2 PREMIER PLUS
Subject: Notification of End of Support for EVIS EUS ENDOSCOPIC ULTRASOUND CENTER Software

Dear Customer

This letter serves as notification of an upcoming change in Olympus' customer support. The effective date shall be the date of issue of the letter. Olympus will no longer provide support for the EVIS EUS Endoscopic Ultrasound Center OLYMPUS EU-ME2 software, including the EU-ME2 Premier* and EU-ME2 Premier Plus models (hereinafter referred to as EU-ME2). This is necessary because the EU-ME2's underlying software components are no longer supported by their vendors.

As of the time of this letter, Olympus has not identified any vulnerabilities in these products and is not aware of any cyber-attacks targeting these products. However, it is important to note that with the termination of support** for the device's software, Olympus will not be able to provide software-based countermeasures to any future vulnerabilities. However, Olympus will disclose if it becomes aware of any exploitation of critical vulnerabilities that affect these products either on our website or communications directly to customers until Olympus terminates the repair service of these devices. Olympus may update the software in the future for specific software components (e.g. capability with other Olympus devices). Such updates would be for functionality rather than cybersecurity.

Recommendations for Future Cyber-Security Risk Mitigation of the EU-ME2

As stated in the IMDRF's Guidance for Medical Device Cybersecurity, stakeholders (e.g., medical device manufacturers (MDM) and healthcare delivery organizations (HDO)) within the healthcare industry have a shared responsibility to provide for the security of medical devices. Olympus recommends that customers continue to follow cybersecurity best practices to secure their environment, such as, but not limited to access-control mechanisms, user procedures, and training to adequately protect medical products from unauthorized access.

Additionally, please consider the following control measures.

- Sealing the USB ports (portable memory port, STORAGE MEMORY terminal)

  Plug in a port lock which cannot be removed without using a dedicated key device (e.g., USB Port Lock, model number: UL03, sold by SmartKeeper or equivalent product), into the portable memory port on the front of the product and the STORAGE MEMORY terminal on the back.

- Sealing the communication terminals (D.FILE terminal, EVIS terminal)

  Apply a sticker that will leave a trace of tampering when removed (e.g., security sticker sold by Sanwa Supply, model number: 200-SL007 or equivalent) to the D.FILE terminal and EVIS terminal on the back of the product.

- Sealing the network terminal (OPTION terminal)

  Plug in a port lock that cannot be removed without using a dedicated key device (e.g., LAN Port Lock sold by SmartKeeper, model number: NL03 or equivalent) into the OPTION terminal on the back of the product.

If you have questions, concerns, or are interested in upgrading to the latest EVIS EUS ENDOSCOPIC ULTRASOUND CENTER, please reach out to your Olympus sales representative or Customer Service Center for more information.

Olympus recommends customers to regularly visit our Product Security websites to obtain the latest product security related information.

*Note: EU-ME2 PREMIER may not be available in some areas.
**Note: Hardware support, such as parts replacement, etc. will continued to be offered.