URGENT MEDICAL DEVICE CORRECTION

GE Healthcare
3000 N. Grandview Blvd. - W440
Waukesha, WI 53188, USA

<Date of Letter Deployment>

GEHC Ref# 34101

To: Chief of Anesthesia
Director of Biomedical / Clinical Engineering
Chief Information Security Officer
Health Care Administrator / Risk Manager

RE: **ICS Advisory - Security Vulnerability of certain GE Anesthesia Systems if connected to an insufficiently secured terminal server**

This document contains important information for your product. Please ensure that all potential users in your facility are made aware of this safety notification and the recommended actions. Please retain this document for your records.

Safety Issue

In an ICS Medical Advisory (ICSMA-19-190-01)[1] issued July 9, 2019, certain Aespire and Aestiva Anesthesia Systems were noted to have a theoretical vulnerability to a cyber-attack when connected to the hospital network. Although extremely improbable, an insufficiently secured terminal server may provide an opportunity for a malicious actor that has already penetrated the hospital network to send fraudulent flow sensor correction parameters. A terminal server is an accessory that can be obtained from a third-party supplier (non-GE Healthcare) outside of the standard product configuration. If fraudulent flow sensor correction parameters are sent, the flow sensor calibration could be impacted and cause over-delivery of tidal volume to a patient if Volume Control ventilation is being used. Over-delivery of tidal volume could in rare cases theoretically lead to an increased risk of lung injury. In addition, under-delivery could theoretically occur and cause too little total volume of gas to be delivered. If this were to occur without normal clinical intervention, there could theoretically be compromise of patient oxygenation or ventilation. There have been no incidences of cyber-attack or injury reported as a result of this issue.

Note: Pressure limits, CO_2 monitoring and bellows movement protective features are not affected and continue to work normally.

REF1: ICS Advisory available at https://ww.us-cert.gov/ics/advisories/icsma-19-190-01

Safety Instructions

You can continue to use your product. If you choose to connect GE Healthcare anesthesia device serial ports to TCP/IP networks, ensure that sufficiently secured terminal servers are used. Secure terminal servers provide robust security features that will prevent this issue.

Affected Product Details

GE Healthcare Anesthesia Systems as follows:
Aespire 7100/100/Protiva/Carestation (Software Version 1.x) - manufactured before October 2010
Aestiva 7100 (Software Version 1.x) -manufactured before February 2014

Aestiva 7900 (Software Version 1.x, 2.x and 3.x) – manufactured before March 2004
Aestiva MRI (Software Version 3.x) – manufactured before July 2014

Contact Information

If you have any questions or concerns regarding this notification, please contact GE Healthcare Service or your local Service Representative. Please complete and return the attached "Customer Response" form via e-mail to RECALL34101.CYBERSECURITY@ge.com.

Please be assured that maintaining a high level of safety and quality is our highest priority. If you have any questions, please contact us immediately per the contact information above.

Sincerely,

GE Healthcare

GE Healthcare

GE Healthcare

GEHC Ref# 34101

MEDICAL DEVICE NOTIFICATION ACKNOWLEDGEMENT
RESPONSE REQUIRED

Please complete this form and return it to GE Healthcare promptly upon receipt and no later than 30 days from receipt. This will confirm receipt and understanding of the Medical Device Correction Notice Ref# 34101.

Customer/Consignee Name: _____

Street Address: _____

City/State/ZIP/Country: _____

Email Address: _____

Phone Number: _____

☐ We acknowledge receipt and understanding of the accompanying Medical Device Notification, and that we have informed appropriate staff and have taken and will take appropriate actions in accordance with that Notification.

Please provide the name of the individual with responsibility who has completed this form.

Signature: _____

Printed Name: _____

Title: _____

Date (DD/MM/YYYY): _____

Please return completed form scanning or taking a photo of the completed form e-mailing to:
RECALL34101.CYBERSECURITY@ge.com
You may obtain this e-mail address through the QR code below: