Johnson&Johnson
MedTech

Abiomed Inc.
22 Cherry Hill Dr,
Danvers, MA 01923 USA

T +1 (978) 646-1400
OneMD-Field-Actions@its.jnj.com
ra-abm-fieldaction@its.jnj.com
www.abiomed.com

URGENT MEDICAL DEVICE CORRECTION

AIC Cybersecurity Notification

Product Code(s)	Product Description(s)	UDI-DI(s)	Impacted Serial Numbers
0042-0000-US	Impella Controller, Packaged, US	00813502010022	All
0042-0010-US	Impella Optical controller, Packaged, US	00813502010985	
0042-0040-US	Optical, AIC, Impella Connect, Pkgd, US	00813502011401	
1000432	AIC w/Impella Connect for ECP	00813502013030	
1000201	Dbl Optical, AIC Impella Connect, Pkg US	00813502010442	

PLEASE DISTRIBUTE THIS INFORMATION TO BIOMEDICAL ENGINEERING, IT DEPARTMENT, AND OTHER APPROPRIATE PERSONNEL AT YOUR FACILITY WHO MAY USE THE PRODUCT THAT IS THE SUBJECT OF THIS NOTICE

Dear Valued Customer,

Please be advised that Abiomed, Inc ("Abiomed") has initiated a voluntary medical device recall (correction) to notify customers of cybersecurity vulnerabilities related to the operating system in the Automated Impella Controller ("AIC") that were discovered through internal routine cybersecurity risk assessments. **Product is not being removed, and hospital inventory can continue to be used.**

REASON FOR NOTIFICATION:

Abiomed has identified cybersecurity vulnerabilities that have residual risk related to network and physical access that could be compromised and that result in uncontrolled risks affecting the Automated Impella Controller (AIC) Operating System. If the identified cybersecurity vulnerabilities are exploited, it may affect the essential performance of the compromised AIC. This may potentially result in loss of device control or unexpected pump stop, which may result in a life-threatening injury, permanent impairment or death.

To date, NO cybersecurity incidents or harm to patients have been reported, and NO life-threatening injury, permanent impairment or death have been reported in relation to the identified vulnerabilities. Healthcare providers can continue to use the AIC as intended.

NEXT STEPS:

- Product is NOT being removed, and hospital inventory can continue to be used.

  Note to Hospital Departments: All vulnerabilities assessed are from the Operating System within the AIC and do not extend beyond the console itself. Our risk assessment has not identified any risks of these AIC vulnerabilities to hospital networks. If you have questions regarding this notice as you perform your hospital network risk assessments, please contact https://www.productsecurity.jnj.com/.

- Keep the AIC in a secure environment with restricted access whether in clinical use or not.

- To mitigate the vulnerability risk, your Abiomed field representative will contact you to arrange disabling the AIC's network capabilities. The AIC may continue to be used as intended.

  If you elect to initiate disabling of the AIC's network capabilities prior to an Abiomed field representative contacting you, you must reach out via ra-abm-fieldaction@its.jnj.com or to your local clinical field staff for instructions. Please note a clinical field staff will need to ensure all steps have been taken if you decide to self- initiate disabling.

DISABLING THE AIC'S NETWORK CAPABILITIES WILL NOT AFFECT THE FUNCTION OF THE AIC OR THE IMPELLA HEART PUMP. THE REMOTE VIEWING CAPABILITIES THROUGH IMPELLA CONNECT WILL BE UNAVAILABLE FOR A PERIOD OF TIME. WE WILL CONTINUE TO INFORM YOU OF ANY PERTINENT INFORMATION.

- Review this notice carefully, and forward to anyone in your facility that needs to be informed including Biomedical Engineering, IT Department, and those who manage, transport, store, stock, or use the AIC.
- If the AIC has been forwarded to another facility, contact that facility and provide them with this notice.

Please note that the following physical controls will remain in place after disabling the network capabilities:

1. The AIC ethernet port and data download via USB is disabled during clinical use.
2. Backup AIC is available per Instructions for Use (IFU).
3. USB port is inactive during patient therapy.

ACTIONS TO BE TAKEN BY CUSTOMER/USER:

- Review, complete all fields, sign, and return the business response form (BRF) provided to impacted customers and send it to Abiomed7920@sedgwick.com.
- If there is suspicion of a cybersecurity event, report to https://www.productsecurity.jnj.com/
- As with any medical device, adverse reactions or quality problems experienced with the use of this product should be reported to the FDA's MedWatch Adverse Event Reporting Program as per below instructions:
    - Complete and submit the report online: www.fda.gov/medwatch/report.htm or
    - Regular Mail or Fax: Download form www.fda.gov/MedWatch/getforms.htm or call 1-800-332-1088 to request a reporting form, then complete and return to the address on the pre-addressed form or submit by fax to 1-800-FDA-0178.

Abiomed is working on security updates and measures to address these cybersecurity vulnerabilities. More information will be provided when further mitigations are available to be deployed to resume network enablement. Abiomed routinely monitors cybersecurity vulnerabilities and will continue to inform you of significant new information if applicable.

At Abiomed, our priority is to our customers and their patients, and that includes the safe and effective use of our products. If you have questions or concerns regarding this notice, please contact ra-abm-fieldaction@its.jnj.com or your local clinical field staff. Thank you for your cooperation.